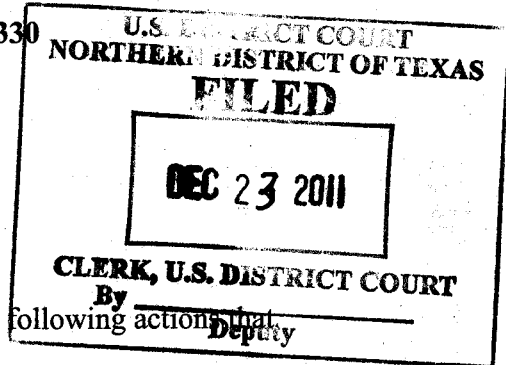


BEFORE THE
UNITED STATES JUDICIAL PANEL ON
MULTIDISTRICT LITIGATION

In re Carrier IQ, Inc.
Consumer Privacy Litigation

MDL No. 2330



NOTICE OF RELATED ACTIONS

Defendant HTC, America, Inc. hereby gives notice of the following actions that are related to MDL No. 2330:

- *Wolff, et al. v. Carrier IQ, Inc., et al.* No. 11-10076
(C.D. Cal. filed Dec. 5, 2011)
- *Olivares, et al. v. Carrier IQ, Inc., et al.* No. 11-6151
(N.D. Cal. filed Dec. 6, 2011)
- *Phong v. Carrier IQ, Inc., et al.* No. 11-6333
(N.D. Cal. filed Dec. 13, 2011)
- *Siegel v. Carrier IQ, Inc., et al.* No. 11-8791
(N.D. Ill. filed Dec. 12, 2011)
- *Cerrone v. Carrier IQ, Inc., et al.* No. 11-5994
(E.D.N.Y. filed Dec. 8, 2011)
- *Accident Investigative Servs., Inc. v. Carrier IQ, Inc., et al.* No. 11-7542
(E.D. Pa. filed Dec. 8, 2011)
- *Lucarelli v. Carrier IQ, Inc., et al.* No. 11-3483
(N.D. Tex. filed Dec. 15, 2011)
- *Kacmarcik v. Carrier IQ, Inc., et al.* No. 11-1119
(E.D. Wis. filed Dec. 9, 2011)

Copies of the complaints and docket sheets for the above-listed actions are attached hereto as Exhibits 1-8.

Respectfully submitted this 21st day of December, 2011.

/s/ Rosemarie T. Ring

Rosemarie T. Ring
Munger, Tolles & Olson LLP
560 Mission Street, 27th Floor
San Francisco, CA 94105
(415) 512-4000
Rose.Ring@mto.com
Counsel for HTC America, Inc.

**BEFORE THE UNITED STATES JUDICIAL PANEL
ON MULTIDISTRICT LITIGATION**

IN RE CARRIER IQ, INC.)
CONSUMER PRIVACY LITIGATION)
_____)

MDL NO. 2330

SCHEDULE OF ACTIONS

	Case Caption	Court	Case No.	Judge
1	Plaintiffs: Caryl Wolff Matthew Fosson Elizabeth Fosson Defendants: Carrier IQ, Inc. HTC America, Inc. HTC Corporation Samsung Electronics America, Inc. Samsung Telecommunications America, Inc.	C.D. Cal.	No. 11-10076	Gary A. Feess
2	Plaintiffs: Israel Olivares Clarissa Portales Defendants: Carrier IQ, Inc. HTC America, Inc.	N.D. Cal.	No. 11-6151	Howard R. Lloyd (U.S.M.J.)
3	Plaintiff: Dao Phong Defendants: Carrier IQ, Inc. HTC America, Inc.	N.D. Cal.	No. 11-6333	Howard R. Lloyd (U.S.M.J.)

	Case Caption	Court	Case No.	Judge
4	Plaintiff: Michael Siegel Defendants: Carrier IQ, Inc. HTC America, Inc. Sprint-Nextel Corporation Samsung Electronics America, Inc.	N.D. Ill.	No. 11-8791	Ronald A. Guzman
5	Plaintiff: Kristina Cerrone Defendants: Carrier IQ, Inc. HTC, Inc. HTC America, Inc.	E.D.N.Y.	No. 11-5994	Roslynn R. Mauskopf
6	Plaintiff: Accident Investigative Services, Inc. Defendants: Carrier IQ, Inc. HTC, Inc. HTC America, Inc.	E.D. Pa.	No. 11-7542	Timothy J. Savage
7	Plaintiff: Richard Lucarelli Defendants: Carrier IQ, Inc. HTC Corporation HTC America, Inc.	N.D. Tex.	No. 11-3483	Barbara M.G. Lynn
8	Plaintiff: Andy Kacmarcik Defendants: Carrier IQ, Inc. HTC America, Inc. HTC Corporation Sprint Nextel Corporation	E.D. Wis.	No. 11-1119	Rudolph T. Randa

**BEFORE THE
UNITED STATES JUDICIAL PANEL ON
MULTIDISTRICT LITIGATION**

IN RE: CARRIER IQ, INC., CONSUMER PRIVACY LITIGATION MDL Docket No. 2330

PROOF OF SERVICE

I hereby certify that a copy of the documents entitled:

**NOTICE OF RELATED ACTIONS
SCHEDULE OF ACTIONS
PROOF OF SERVICE**

were filed via ECF. The documents will be served by Federal Express on December 22, 2011, on the following:

Clerk, United States District Court Eastern District of Pennsylvania (Philadelphia) 601 Market Street, Room 2609 Philadelphia, PA 19106-1797 Telephone: (215) 597-7704 2:11-cv-07542-TJS	Clerk, United States District Court Eastern District of Wisconsin 362 United States Courthouse 517 East Wisconsin Avenue Milwaukee, WI 53202 Telephone: (414) 297-3372 2:11-cv-01119-RTR
Clerk, United States District Court Eastern District of New York 225 Cadman Plaza East Brooklyn, NY 11201 Telephone: (718) 613-2600 1:11-cv-05994-RRM-JMA	Clerk, United States District Court Northern District of Texas 1100 Commerce St., Room 1452 Dallas, Texas 75242 Telephone: (214) 753-2200 3:11-cv-03483-M
Clerk, United States District Court Northern District of California (San Jose) 280 South 1 st Street San Jose, CA 95113 Telephone: (408) 535-5363 5:11-cv-06151-HRL 5:11-cv-06333-HRL	Clerk, United States District Court Northern District of Illinois Everett McKinley Dirksen United States Courthouse 219 South Dearborn Street Chicago, IL 60604 Telephone: (312) 435-5670 1:11-cv-08791

Clerk, United States District Court Central District of California 312 N. Spring Street Los Angeles, CA 90012 Telephone: (213) 894-1565 2:11-cv-10076-GAF-MRW	
--	--

The documents will also be served by electronic mail on December 21, 2011, on the following:

Counsel	Plaintiff	Jurisdiction	Case No.
Charles E. Schaffer Levin, Fishbein, Sedran & Berman 510 Walnut Street Suite 500 Philadelphia, Pa 19106 215-592-1500 cschaffer@lfsblaw.com	Accident Investigative Services, Inc.	Eastern District of Pennsylvania (Philadelphia)	2:11-cv-07542-TJS
Michael M. Weinkowitz Levin Fishbein Sedran & Berman 510 Walnut Street Suite 500 Philadelphia, PA 19106 215-592-1500 Fax: 215-592-4663 mweinkowitz@lfsblaw.com	Kristina Cerrone	Eastern District of New York	1:11-cv-05994-RRM-JMA

<p>Ben Barnow Blake A Strautins Barnow and Associates PC 1 N LaSalle St – Ste 4600 Chicago, IL 60602 312-621-2000 Fax: 312-641-5504 b.barnow@barnowlaw.com b.strautins@barnowlaw.com</p> <p>David J Syrios Guri Ademi Shpetim Ademi Ademi & O'Reilly LLP 3620 E Layton Ave Cudahy, WI 53110 414-482-8000 Fax: 414-482-8001 dsyrios@ademilaw.com gademi@ademilaw.com sademi@ademilaw.com cmather@ademilaw.com</p>	<p>Andy Kacmarcik</p>	<p>Eastern District of Wisconsin (Milwaukee)</p>	<p>2:11-cv-01119-RTR</p>
<p>David M Finn Milner Finn Price 2828 N Harwood Suite 1950 Dallas, TX 75201 214/651-1121 Fax: 214/953-1366 judgefinn@davidfinn.com</p>	<p>Richard Lucarelli</p>	<p>Northern District of Texas</p>	<p>3:11-cv-03483-M</p>
<p>Brian R Strange Strange and Carpenter 12100 Wilshire Boulevard Suite 1900 Los Angeles, CA 90025 310-207-5055 Fax: 310-826-3210 lacounsel@earthlink.net</p> <p>Joseph H Malley Law Office of Joseph H. Malley, PC 1045 North Zang Boulevard Dallas, TX 75208 214-943-6100 malleylaw@gmail.com</p>	<p>Israel Olivares</p>	<p>California Northern District (San Jose)</p>	<p>5:11-cv-06151-HRL</p>

Mark Punzalan Finkelstein, Thompson LLP 100 Bush Street Suite 1450 San Francisco, CA 94104 415-398-8700 Fax: 415-398-8704 mpunzalan@finkelsteinthompson.com	Dao Phong	California Northern District (San Jose)	5:11-cv-06333-HRL
Larry D. Drury Larry D. Drury, Ltd. 100 N. LaSalle St. Suite 1010 Chicago, IL 60602 (312) 346-7950 ldrurylaw@aol.com	Michael Siegel	Northern District of Illinois	1:11-cv-08791
Brian C Gudmundson David M Cialkowski Zimmerman Reed PLLP 801 South Figueroa Street Minneapolis, MN 55402 612-341-0400 Fax: 612-341-0844 brian.gudmundson@zimmreed.com david.cialkowski@zimmreed.com Daniel Lawrence Germain Rosman & Germain LLP 16311 Ventura Boulevard Suite 1200 Encino, CA 91436-2152 818-788-0877 Fax: 818-788-0885 germain@lalawyer.com Paula M Roach Timothy G Blood Blood Hurst & O'Reardon LLP 600 B Street Suite 1550 San Diego, CA 92101-3301 619-338-1100 Fax: 619-338-1101 proach@bholaw.com tblood@bholaw.com	Caryl Wolff Matthew Fosson Elizabeth Fosson	United States District Court, Central District of California (Western Division - Los Angeles)	2:11-cv-10076-GAF-MRW

DATED: December 21, 2011

/s/ Susan Ahmadi

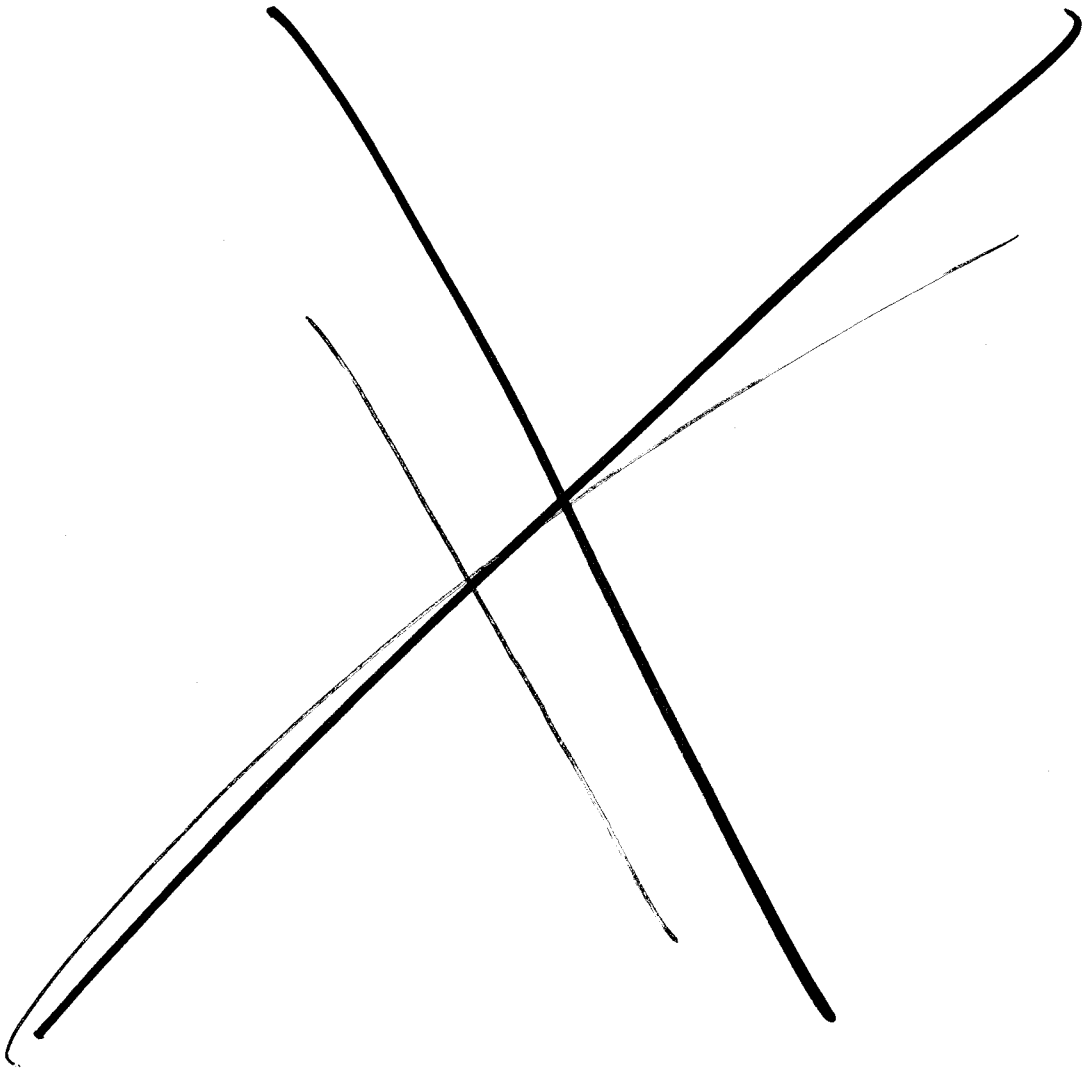


Exhibit 1:

Wolff, et al. v. Carrier IQ, Inc., et al.

(MRWx), DISCOVERY

**UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA
(Western Division - Los Angeles)
CIVIL DOCKET FOR CASE #: 2:11-cv-10076-GAF-MRW**

Caryl Wolff v. Carrier IQ Inc et al
Assigned to: Judge Gary A. Feess
Referred to: Magistrate Judge Michael R. Wilner
Cause: 18:2510 Wire Interception

Date Filed: 12/05/2011
Jury Demand: Plaintiff
Nature of Suit: 890 Other Statutory
Actions
Jurisdiction: Federal Question

Plaintiff

Caryl Wolff
*individually and on behalf of all others
similarly situated*

represented by **Brian C Gudmundson**
Zimmerman Reed PLLP
801 South Figueroa Street
Minneapolis, MN 55402
612-341-0400
Fax: 612-341-0844
Email: brian.gudmundson@zimmreed.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

Daniel Lawrence Germain
Rosman & Germain LLP
16311 Ventura Boulevard Suite 1200
Encino, CA 91436-2152
818-788-0877
Fax: 818-788-0885
Email: germain@lalawyer.com
ATTORNEY TO BE NOTICED

David M Cialkowski
Zimmerman Reed PLLP
1100 IDS Center
80 South Eighth Street
Minneapolis, MN 55402
612-341-0400
Fax: 612-341-0844
Email: david.cialkowski@zimmreed.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

Paula M Roach
Blood Hurst & O'Reardon LLP
600 B Street Suite 1550
San Diego, CA 92101-3301
619-338-1100
Fax: 619-338-1101
Email: proach@bholaw.com
ATTORNEY TO BE NOTICED

Timothy G Blood
Blood Hurst & O'Reardon LLP
600 B Street Suite 1550
San Diego, CA 92101
619-338-1100
Fax: 619-338-1101
Email: tblood@bholaw.com
ATTORNEY TO BE NOTICED

Plaintiff

Matthew Fosson
individually and on behalf of all others
similarly situated

represented by **Matthew Fosson**
 PRO SE

Plaintiff

Elizabeth Fosson
individually and on behalf of all others
similarly situated

represented by **Elizabeth Fosson**
 PRO SE

V.

Defendant

Carrier IQ Inc
a Delaware corporation

Defendant

HTC Corporation
a Taiwanese corporation

Defendant

HTC America Inc
a Washington corporation

Defendant

Samsung Electronics America, Inc.
a New York corporation

Defendant

Samsung Telecommunications America Inc.
a Delaware corporation

Date Filed	#	Docket Text
12/05/2011	<u>1</u>	CLASS ACTION COMPLAINT against Defendants Carrier IQ Inc, HTC America Inc, HTC Corporation. Case assigned to Judge Gary A. Feess for all further proceedings. Discovery referred to Magistrate Judge Michael R Wilner.(Filing fee \$ 350 Paid.) Jury Demanded., filed by Plaintiff Caryl Wolff. (et) (mg). (Entered: 12/07/2011)
12/05/2011		21 DAY Summons Issued re Complaint – (Discovery) <u>1</u> as to Defendants Carrier IQ Inc, HTC America Inc, HTC Corporation. (et) (Entered: 12/07/2011)
12/05/2011	<u>2</u>	CERTIFICATION AND NOTICE of Interested Parties filed by Plaintiff Caryl Wolff. (et) (mg). (Entered: 12/07/2011)
12/07/2011	<u>3</u>	NOTICE OF FILING FEE DUE on Pro Hac Vice Application mailed to David M. Cialkowski for Plaintiff Caryl Wolff. Your Pro Hac Vice application has not been received by the court. Please return your completed Application of Non-Resident Attorney to Appear in a Specific Case, form G-64, or a copy of the Notice of Electronic Filing of your application and the \$325.00 fee and this notice immediately. Out-of-state federal government attorneys who are not employed by the U.S. Department of Justice are required to file a Pro Hac Vice application; no filing fee is required. (et) (Entered: 12/07/2011)
12/07/2011	<u>4</u>	NOTICE OF FILING FEE DUE on Pro Hac Vice Application mailed to Brian C. Gudmundson for Plaintiff Caryl Wolff. Your Pro Hac Vice application has not been received by the court. Please return your completed Application of Non-Resident Attorney to Appear in a Specific Case, form G-64, or a copy of the Notice of Electronic Filing of your application and the \$325.00 fee and this notice immediately. Out-of-state federal government attorneys who are not employed by

		the U.S. Department of Justice are required to file a Pro Hac Vice application; no filing fee is required. (et) (Entered: 12/07/2011)
12/13/2011	<u>5</u>	CERTIFICATION of Interested Parties filed by Plaintiff Caryl Wolff, (bp) (Entered: 12/15/2011)
12/13/2011	<u>6</u>	FIRST AMENDED COMPLAINT against defendants Carrier IQ Inc, HTC America Inc, HTC Corporation, Samsung Electronics America, Inc., Samsung Telecommunications America Inc. amending Complaint – (Discovery), <u>1</u> , filed by plaintiffs Caryl Wolff, Matthew Fosson, Elizabeth Fosson (bp) (Additional attachment(s) added on 12/20/2011: # <u>1</u> summons issued) (bp). (Entered: 12/16/2011)
12/13/2011		21 DAY Summons Issued re Amended Complaint, <u>6</u> as to Defendants Carrier IQ Inc, HTC America Inc, HTC Corporation, Samsung Electronics America, Inc., Samsung Telecommunications America Inc.. (bp) (Entered: 12/20/2011)
12/16/2011	<u>8</u>	APPLICATION for attorney Brian C. Gudmundson to Appear Pro Hac Vice. (PHV FEE PAID.) filed by plaintiff Caryl Wolff. Lodged Proposed Order. (bp) (Entered: 12/19/2011)
12/19/2011	<u>7</u>	APPLICATION for attorney David M. Cialkowski to Appear Pro Hac Vice. (PHV FEE PAID.) filed by plaintiff Caryl Wolff. Lodged Lodged Order. (bp) (Entered: 12/19/2011)
12/19/2011	<u>9</u>	ORDER by Judge Gary A. Feess granting <u>7</u> Application to Appear Pro Hac Vice by Attorney David Cialkowski on behalf of plaintiff, designating Daniel Germain as local counsel. (ak) (Entered: 12/20/2011)
12/19/2011	<u>10</u>	ORDER by Judge Gary A. Feess: granting <u>8</u> Application to Appear Pro Hac Vice by Attorney Brian Gudmundson on behalf of plaintiff, designating Daniel Germain as local counsel. (ak) (Entered: 12/20/2011)

Daniel L. Germain (Bar No. 143334)
ROSMAN & GERMAIN LLP
16311 Ventura Blvd., Suite 1200
Encino, CA 91436-2152
Telephone: (818) 788-0877
Facsimile: (818) 788-0885
E-Mail: R&G@Lalawyer.com

David M. Cialkowski
Brian C. Gudmundson
ZIMMERMAN REED, PLLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
E-Mail: david.cialkowski@zimmreed.com

Additional Counsel Listed on Signature Page

Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CARYL WOLFF, MATTHEW
FOSSON, ELIZABETH FOSSON,
individually and on behalf of all others
similarly situated,

Plaintiffs,

vs.

CARRIER IQ, INC., a Delaware
corporation; HTC CORPORATION, a
Taiwanese corporation; HTC
AMERICA, INC., a Washington
corporation; SAMSUNG
ELECTRONICS AMERICA, INC., a
New York corporation; SAMSUNG
TELECOMMUNICATIONS
AMERICA, INC., a Delaware
corporation.

Defendants.

Case No.: CV11-10076 GAF (MRWx)

**FIRST AMENDED CLASS ACTION
COMPLAINT**

1. VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. §§ 1830 *et seq.*;
2. VIOLATION OF THE FEDERAL WIRETAP ACT AS AMENDED BY THE ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. §§ 2510, *et seq.*;
3. VIOLATION OF CALIFORNIA'S COMPUTER CRIME LAW, California Penal Code §§ 502, *et seq.*;
4. VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT, California Penal Code §§ 630 *et seq.*;
5. VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW, California Business and Professions Code §§ 17200, *et seq.*; and
6. VIOLATION OF CALIFORNIA'S CONSUMERS LEGAL REMEDIES ACT, California Civil Code §§ 1750, *et seq.*

DEMAND FOR JURY TRIAL

2011 DEC 13 PM 2:49
CLERK U.S. DISTRICT COURT
CENTRAL DISTRICT OF CALIF.
LOS ANGELES

FILED

1 Plaintiffs bring this action individually and on behalf of a class of similarly situated
2 consumers who purchased cellular telephones embedded with software capable of
3 tracking, recording and transmitting personal and private information. Plaintiffs bring this
4 action against Carrier IQ, Inc., who developed the software, and Defendants HTC
5 Corporation, HTC America, Inc., Samsung Electronics America, Inc., and Samsung
6 Telecommunications America, Inc., the cellular telephone manufacturers who knowingly
7 embedded their phone products with the software, or allowed it to be embedded.

8 INTRODUCTION

9 1. Carrier IQ ("CIQ") designs, develops, and markets software capable of
10 tracking, recording and transmitting electronic data to cellphone service providers or other
11 CIQ customers. CIQ boasts that its software is currently running on over 141 million
12 cellular telephones ("cellphones").

13 2. CIQ's software, once installed on a cellphone, surreptitiously runs in the
14 background, capturing and logging the activities of the cellphone user. The software
15 functions by recording the key strokes of the user and transmitting that data to a separate
16 location which can be accessed by cellphone service providers.

17 3. The content of the information recorded CIQ's application is very personal
18 and private. This information includes, but is not limited to:

- 19 a. When users turn their phones on and off;
- 20 b. The phone numbers users dial;
- 21 c. The contents of the text messages users receive;
- 22 d. The URLs of the websites users visit;
- 23 e. The contents of users' online search queries; and
- 24 f. The location of the customer using the smartphone – even when the customer
25 has *expressly denied* permission for that information to be recorded.

26 4. By embedding the CIQ software in Plaintiffs' cellphones and capturing,
27 recording, and transmitting personal electronic data, Defendants have directly violated
28 applicable federal and state law.

1 5. Plaintiffs seek to stop Defendants' unauthorized and illegal interception of
2 electronic communications and to recover damages and other relief prescribed by law.

3 **JURISDICTION**

4 6. This Court has subject matter jurisdiction over this action under 28 U.S.C. §
5 1331 in that Plaintiffs allege violations of federal law, namely the Federal Wiretap Act as
6 amended by the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 *et seq.*, and
7 the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1830 *et seq.* The Court has supplemental
8 jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367(a).

9 7. This Court has personal jurisdiction over the Defendants in this action due to
10 the fact that Defendants are licensed to do business in the state of California or otherwise
11 conduct business in the state of California.

12 8. Venue is proper in the Court pursuant to 28 U.S.C. § 1291(b)(2) because a
13 substantial part of the events giving rise to this claim have occurred in this district and
14 Defendants regularly conduct business in this district.

15 **PARTIES**

16 9. Plaintiff Caryl Wolff is a resident of the City of Los Angeles, State of
17 California. Caryl Wolff purchased and uses a cellphone manufactured by HTC embedded
18 with CIQ's software. Plaintiff Caryl Wolff has suffered injury in fact and lost money or
19 property as a result of the conduct alleged. Defendants have taken her personal, private
20 information for commercial purposes without her consent or agreement and otherwise
21 without legal authority to do so.

22 10. Plaintiff Matthew Fosson is a resident of the City of Lawrenceburg, State of
23 Kentucky. Matthew Fosson purchased and used a cellphone manufactured by HTC
24 embedded with CIQ's software. Plaintiff Mathew Fosson has suffered injury in fact and
25 lost money or property as a result of the conduct alleged. Defendants have taken his
26 personal, private information for commercial purposes without his consent or agreement
27 and otherwise without legal authority to do so.
28

11. Plaintiff Elizabeth Fosson is a resident of the City of Lawrenceburg, State of Kentucky. Elizabeth Fosson purchased and used a cellphone manufactured by Samsung embedded with CIQ's software. Plaintiff Elizabeth Fosson has suffered injury in fact and lost money or property as a result of the conduct alleged. Defendants have taken his personal, private information for commercial purposes without her consent or agreement and otherwise without legal authority to do so.

12. Defendant Carrier IQ, Inc., is a Delaware corporation, headquartered in Mountain View, California. Carrier IQ develops, markets and distributes software designed to record, track and transmit cellphone users' personal data.

13. Defendant HTC Corporation ("HTC") is a Taiwan corporation and a cellphone manufacturer location in Taoyuan, Taiwan. HTC has offices within the United States and sells its products throughout the United States, including throughout California. It is also the parent company of Defendant HTC America, Inc.

14. Defendant HTC America, Inc. ("HTC America") is a Washington corporation with its principal place of business in Bellevue, Washington. HTC America sells its products throughout the United States, including throughout California.

15. Defendant Samsung Electronics America, Inc. ("Samsung Electronics") is a New York corporation with its principal place of business in Ridgefield Park, New Jersey. Samsung Electronics has offices within the United States and sells its products throughout the United States, including throughout California.

16. Defendant Samsung Telecommunications America, Inc. ("Samsung Telecommunications") is a Delaware Corporation with its principal place of business in Richardson, Texas. Samsung Telecommunications has offices within the United States and sells its products throughout the United States, including throughout California.

FACTUAL BACKGROUND

A. Carrier IQ

17. Carrier IQ is the "world's leading provider of Mobile Service Intelligence solutions." CIQ develops software that tracks and delivers "data drawn directly from []

1 subscribers' devices" to provide "detailed insight into the mobile experience as delivered
2 at the handset. . . ."

3 18. Carrier IQ has created a suite of data tracking software which it markets to
4 cellphone service providers, among others, who find it valuable to be able to get a "precise
5 view" of a customer's interaction with their cellphone.

6 19. One of Carrier IQ's most successful applications is the IQ Insight Experience
7 Manager ("CIQ's Software"). Carrier IQ's online data sheet explains why:

8 IQ Insight Experience Manager provides a level of visibility into true
9 customer experience, previously unavailable in the mobile industry. Based on
10 Carrier IQ's leading Mobile Service Intelligence Technology, IQ Insight
11 Experience Manager uses data directly from the mobile phone itself to give a
12 precise view of how users interact with both their phones and the service
13 delivered through them, even if the phone is not communicating with the
14 network.

15 20. CIQ's Software gives carriers detailed views of how customers interact with
16 their phones at "any level of granularity from the entire population, to comparative groups,
17 down to individual users, all at the touch of a button."

18 **B. Operation of CIQ's Software**

19 21. CIQ's Software functions as a rootkit. A rootkit is software that enables
20 continued privileged access to a computer while actively hiding its presence from
21 administrators, like Plaintiffs, by subverting standard operating system functions and other
22 applications.

23 22. CIQ's Software operates by monitoring for commands called "triggers." For
24 example, a user opening an application on their cellphone can be a trigger for the CIQ
25 software to record and transmit information about the text message.

26 23. What actions serve as "triggers" to the CIQ software is predetermined by CIQ
27 and the Cellphone Service Providers. Known triggers on HTC phones, as discovered by
28 third party software developer Trevor Eckhart, include, but are not limited to, (1) when
keys on the phone are pressed, (2) when the user changes physical locations, (3) when the

user taps the screen, and (4) when a user accesses a webpage. Leaked training materials from CIQ show other actions that can "trigger" the CIQ software:

CARRIER		2007-01-05 20:13:21 GMT+07:00. References: logon multiple.do, test
DIS v2.0 References		Device Index
Device	Triggers	Device List
Triggers		
Name	Title	Description
U006	App End	Signals the end of an application
U001	App Start	Signals the launch of an application
AST1	Asset	The trigger for when an asset has occurred
AL17	Browser End	Signals the completion of a page render
AL15	Browser Start	Signals the launch a web page
RF15	CRC Error	A CRC Error occurred
HT10	CNS End	Signals a CNS resolution response
HT17	CNS Start	Signals the request for a CNS resolution
VC00	Data Call Start	The trigger for when a data call starts.
RF14	Data Handoff End	Signals the completion of a data handoff
RF13	Data Handoff Start	Signals a data handoff beginning
DO1E	EVDO Call End	Signals the end of and EVDO call
DO0E	EVDO Call Start	Signals the beginning of a EVDO call
HE01	HTTP Error	The trigger for there is new HTTP error
HT0F	HTTP Request	Signals an HTTP Request
HT10	HTTP Response	Signals an HTTP Response
EA01	ARM Hardware Exception	The trigger for when a hardware exception from the previous power cycle has been reported upon bootup
NT09	IP Session End	Signals the end of and IP session
NT08	IP Session Start	Signals the start of an IP session
AL03	Java End	Signals an Java transaction has completed
AL01	Java Start	Signals Java transaction starting
AL19	Java Download	Trigger for when a Java app is downloaded
HT0E	Mio Start	The trigger for when a MIP Session starts.
VC00	Traffic Call Start	
VC0E	Voicemail Call Start	

1 24. Once triggered, the CIQ software records certain information. This
2 information is then sent to another location named the Carrier IQ Portal where the
3 information is organized and stored.

4 25. At the Carrier IQ Portal, devices are displayed by individual phone
5 Equipment ID and Subscriber IDs. Portal Administrators can organize the information and
6 subdivide the data sets further depending on their needs.

7 **C. CIQ Software Records Private Information And Degrades The**
8 **Performance of Cellphones.**

9 26. CIQ software was embedded in millions of cellphones around the world,
10 including cellphones manufactured by HTC and Samsung. CIQ software is preinstalled
11 and operates from the time the user begins to use their cellphone.

12 27. On or about November 28, 2011, Mr. Eckhart published an analysis report
13 titled "Carrier IQ Part 2." His report included a 17 minute video in which he offered proof
14 that the CIQ software logged his key strokes, recorded his SMS text messages, recorded
15 dialed numbers, and tracked his internet use, including on HTTPS (secure) websites.

16 28. Mr. Eckhart's report was quickly picked up by the media. Andy Greenberg,
17 reporting for Forbes, wrote:

18
19 As Echart's analysis of the company's training videos and the debugging logs
20 on his own HTC Evo handset have shown, Carrier IQ captures every
21 keystroke on a device as well as location and other data, and potentially
22 makes that data available to Carrier IQ's customers. The video he's created
23 (below) shows every keystroke being sent to the highly-obscured application
24 on the phone before a call, text message, or Internet data package is ever
25 communicated beyond the phone. Eckhart has found the application on
26 Samsung, HTC, Nokia and RIM devices, and Carrier IQ claims on its website
27 that it has installed the program on more than 140 million handsets.

28 29. CIQ has claimed that the information it records is used for service
maintenance purposes only and that no personal or private data is transmitted to cellphone
service providers. However, the patent materials for CIQ's own software, discredit this

1 claim. CIQ's patent for CIQ's software states that it is a "method for collecting data at a
2 server coupled to a communications network. . . ." The patent goes on to state that the data
3 to be collected is that which relates "to an end user's interaction with the device," and
4 states that this interaction is "the end user's pressing of keys on the device."

5 30. CIQ's own marketing materials further show that its software transmits
6 personal and private data to cellphone service providers. The marketing material
7 promoting CIQ's software states:

8 a. The software is able to "capture a vast array of experience data
9 including screen transitions, button presses, service interactions and anomalies."

10 b. The software will allow users to see "application and device feature
11 usage, such as camera, music, messaging, browser, and tv."

12 c. Most disturbingly, that CIQ's software allows users to "[i]dentify
13 exactly how [their] customers interact with services and which ones they use. See
14 which content they consume, even offline."

15 31. In addition, CIQ's software degrades the performance of cellphones. Another
16 Android developer, Tim Schofield, extensively researched the presence of the CIQ
17 software on multiple Android smartphone platforms. He noted that in addition to the
18 privacy issues, the embedded software necessarily degrades the performance of any device
19 on which it is installed. CIQ's software is always operating and cannot be turned off. It
20 necessarily uses system resources, thus slowing performance and decreasing battery life.
21 As a result, because of the CIQ software, in addition to having their private
22 communications intercepted, Plaintiffs and Class Members are not getting the optimal
23 performance of the smartphone devices that they purchased, and which are marketed, in
24 part, based on their speed, performance, and battery life.

25 32. CIQ's practices have garnered the attention of Congress. On November 30,
26 2011, Senator Al Franken, Chairman of the Subcommittee on Privacy, Technology and the
27 Law wrote a letter to CIQ's President and CEO, Larry Lenhart, stating that he was very
28 concerned that CIQ's software is able to track, record and transmit private information.

1 Senator Franken stated that it appeared CIQ software captured a broad swath of extremely
2 sensitive information which had nothing to do with diagnostics. He demanded that CIQ
3 answer numerous questions, including whether CIQ software recorded private data,
4 whether it recorded the data even when the phone was off and whether the private data is
5 subsequently shared with third parties.

6 CLASS ALLEGATIONS

7 33. Plaintiffs bring this action under Rule 23 of the Federal Rules of Civil
8 Procedure, on behalf of themselves and a proposed Class consisting of:

9 All persons in the United States that own or owned HTC or Samsung branded
10 telephones or other devices on which CIQ software was installed or
11 embedded.

12 Excluded from the proposed Class are Defendants; Defendants' affiliates and subsidiaries;
13 Defendants' current or former employees, officers, directors, agents, and representatives;
14 and the judge or magistrate judge to whom this case is assigned, as well as those judges'
15 immediate family members.

16 34. Numerosity: The members of the Class are so numerous that their individual
17 joinder is impracticable. Plaintiffs are informed and believe, and on that basis allege, that
18 the proposed Class contains tens of thousands of members. The precise numbers of Class
19 members is unknown to Plaintiffs. The true numbers of Class members are known by
20 Defendants, however, and thus, may be notified of the pendency of this action by first
21 class mail, electronic mail, and by published notice. Upon information and belief, Class
22 members can be identified through Defendants' the electronic records.

23 35. Commonality: Pursuant to Federal Rules of Civil Procedure, Rule 23(a)(3)
24 and Rule 23(b)(3), commonality and predominance are satisfied because there are
25 questions of law and fact common to Plaintiffs and the Class, which predominate over any
26 individual questions affecting only individual members. The common questions of law
27 and fact include, but are not limited to:

28 a. Whether CIQ software has intercepted, recorded, and retransmitted
Plaintiffs' personal and private information including, but not limited to, SMS text

1 messages, keystrokes, telephone numbers, and other information, without the permission
2 or knowledge of Plaintiffs.

3 b. Whether CIQ and the device manufacturers have violated the Federal
4 Wiretap Act, 18 U.S.C. § 2510 et seq., including the prohibition on the interception,
5 disclosure, and use of wire, oral, or electronic communications, or otherwise, by way of
6 the acts and omissions set forth in this complaint.

7 c. Whether CIQ and the Device Manufacturers have violated the
8 Computer Fraud and Abuse Act, 18 U.S.C. § 1030, by implementing a software program
9 that cannot be removed from Plaintiffs' devices and which operates without Plaintiffs'
10 knowledge and permission.

11 d. Whether CIQ and the Device Manufacturers have violated the
12 California Invasion of Privacy Act, California Penal Code § 630, by embedding a software
13 program that cannot be removed from Plaintiffs' devices and which records Plaintiffs'
14 personal and private data.

15 e. Whether Defendants have violated California's Computer Crime Law,
16 Penal Code § 502, by embedding a software program that cannot be removed from
17 Plaintiffs' devices and which records Plaintiffs' personal and private data.

18 f. Whether CIQ and the Device Manufacturers have violated the
19 California Unfair Business Practices Act, by secretly installing CIQ software in Plaintiffs'
20 cellphones, failing to disclose that the CIQ software degraded the performance and battery
21 life of the devices on which it was installed, failing to disclose that the software degrades
22 the performance and battery life of the cellphone and surreptitiously taking private and
23 confidential information from Plaintiffs and other member of the Class.

24 g. Whether Plaintiffs are entitled to remedies under the California Legal
25 Remedies Act, due to the actions and omissions of Defendants as alleged herein.

26 h. Whether Defendants are liable for statutory and other damages, civil
27 penalties, punitive damages, restitution, and/or whether declaratory or injunctive relief is
28 appropriate.

1 loss to one or more persons during any one-year period aggregating at least \$5,000 in
2 value.

3 41. Plaintiffs' cellphones are "protected computer[s] . . . which are used in
4 interstate commerce and/or communication" within the meaning of 18 U.S.C. §
5 1030(e)(1)-(2).

6 42. Defendants violated 18 U.S.C. § 1030(a)(2)(C) by intentionally accessing
7 Plaintiffs' cellphones, without authorization or by exceeding access, thereby obtaining
8 information from such protected Computing Devices.

9 43. Defendants violated 18 U.S.C. § 1030(a)(5)(A)(iii) by intentionally accessing
10 Plaintiffs' cellphone without authorization, and as a result of such conduct, caused damage
11 and loss to Plaintiffs and Class members.

12 44. Plaintiffs have suffered damage by reason of these violations, as defined in 18
13 U.S.C. § 1030(e)(8), by the "impairment to the integrity or availability of data, a program,
14 a system or information."

15 45. Plaintiffs have suffered loss by reason of these violations, including, without
16 limitation, violation of the right of privacy, disclosure of personal identifying information,
17 sensitive identifying information, and personal information, and interception of
18 transactional information that otherwise is private, confidential, and not of public record.

19 46. As a result of these takings, Defendants' conduct has caused a loss to one or
20 more persons during any one-year period aggregating at least \$5,000 in value in real
21 economic damages.

22 47. Plaintiffs and Class members have additionally suffered loss by reason of
23 these violations, including, without limitation, violation of the right of privacy.

24 48. The CFAA, 18 U.S.C. § 1030 (g), provides a civil cause of action to "any
25 person who suffers damage or loss by reason of a violation" of a CFAA. Defendant
26 Carrier IQ asserts in its marketing materials that, with its software installed on a cellular
27 device, a carrier can: "Identify exactly how your customers interact with services and
28 which ones they use. See which content they consume, even offline." But information

1 about which services consumers use is private. Information about the “content they
2 consume” is private. Consumers own this information, and Defendants have taken it
3 without just compensation. Plaintiffs and Class members seek to be given the monetary
4 value of this private data that was transmitted and sold.

5 49. Defendants’ unlawful access to Plaintiffs’ cellphones and electronic
6 communications has caused Plaintiffs irreparable injury. Unless restrained and enjoined,
7 Defendants will continue to commit such acts. Plaintiffs’ remedy at law is not adequate to
8 compensate it for these inflicted and threatened injuries, entitling Plaintiff to remedies
9 including injunctive relief as provided by 18 U.S.C. § 1030(g).

10 COUNT II
11 VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
12 18 U.S.C. § 2510 *et seq.*

13 50. Plaintiffs incorporate the above allegations by reference as if set forth herein
14 at length.

15 51. The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510,
16 referred to as “ECPA,” regulates wire and electronic communications interception and
17 interception of oral communications, and makes it unlawful for a person to “willfully
18 intercept[], endeavor[] to intercept, or procure[] any other person to intercept or endeavor
19 to intercept, any wire, oral, or electronic communication,” within the meaning of 18 U.S.C.
20 § 2511(1).

21 52. Defendants violated 18 U.S.C. § 2511 by intentionally acquiring and/or
22 intercepting, by device or otherwise, Plaintiffs’ electronic communications, without their
23 knowledge, consent or authorization.

24 53. The contents of data transmissions from and to Plaintiffs’ cellphones
25 constitute “electronic communications” within the meaning of 18 U.S.C. § 2510.

26 54. Plaintiffs and Class Members are “person[s] whose . . . electronic
27 communication is intercepted . . . or intentionally used in violation of this chapter” within
28 the meaning of 18 U.S.C. § 2520.

1 62. Plaintiffs have standing to assert civil causes of action pursuant to California
2 Penal Code § 502(e)(1) which states “[i]n addition to any other civil remedy available, the
3 owner or lessee of the computer, computer system, computer network, computer program,
4 or data who suffers damage or loss by reason of a violation of any of the provisions of
5 subdivision (c) may bring a civil action against the violator for compensatory damages and
6 injunctive relief or other equitable relief.”

7 63. The California Computer Crime Law, California Penal Code § 502, referred
8 to as “CCL” regulates “tampering, interference, damage, and unauthorized access to
9 lawfully created computer data and computer systems.”

10 64. Defendants violated California Penal Code § 502 by knowingly accessing,
11 copying, using, making use of, interfering, and/or altering data belonging to Plaintiffs: (1)
12 in and from the State of California; (2) in the home states of the Plaintiffs; and (3) in the
13 state in which the servers that provided the communication link between Plaintiffs and the
14 websites interacted with were located.

15 65. Pursuant to California Penal Code § 502(b)(1), “Access means to gain entry
16 to, instruct, or communication with the logical, arithmetical, or memory function resources
17 of a computer, computer system, or computer network.”

18 66. Pursuant to California Penal Code § 502(b)(6), “data means a representation
19 of information, knowledge, facts, concepts, computer software, computer programs or
20 instructions. Data may be in any form, in storage media, or as stored in the memory of the
21 computer or in transit or presented on a display device.”

22 67. Pursuant to California Penal Code § 502(b)(8), “Injury means any alteration,
23 deletion, damage, or destruction of a computer system, computer network, computer
24 program, or data caused by the access or the denial of access to legitimate users of
25 computer system, network, or program.”

26 68. Pursuant to California Penal Code § 502(b)(10) a “Computer contaminant
27 system means any set of computer instructions that are designed to modify, damage,
28

1 destroy, record, or transmit information within a computer, computer system, or computer
2 network without the intent or permission of the owner of the information.”

3 69. Defendants have violated California penal Code § 502(c)(2) by knowingly
4 accessing and without permission, taking or making use of data from Plaintiffs’
5 cellphones.

6 70. Defendants have violated California penal Code § 502(c)(3) by knowingly
7 and without permission, using and causing to be used Plaintiffs’ cellphones.

8 71. Defendants have violated California Penal Code § 502(c)(8) by knowingly
9 introducing a computer containment into the Plaintiffs’ Computer Devices to obtain data
10 regarding Plaintiffs’ electronic communications.

11 72. Plaintiffs have additionally suffered loss by reason of these violations,
12 including, a violation of the right of privacy. Defendant Carrier IQ asserts in its marketing
13 materials that, with its software installed on a cellular device, a carrier can: “Identify
14 exactly how your customers interact with services and which ones they use. See which
15 content they consume, even offline.” But information about which services consumers use
16 is private. Information about the “content they consume” is private. Consumers own this
17 information, and Defendants have taken it without just compensation. Plaintiffs and Class
18 members seek to be given the monetary value of this private data that was transmitted and
19 sold.

20 73. As a direct and proximate result of Defendants’ unlawful conduct, Defendants
21 have caused loss to Plaintiffs in an amount to be proven at trial. Plaintiffs are also entitled
22 to recover their reasonable attorneys’ fees pursuant to California Penal Code § 502(e).

23 74. Plaintiffs has also suffered irreparable injury from these unauthorized acts of
24 disclosure, to wit: all of their personal, private, and sensitive electronic communications
25 have been harvested, viewed, accessed, stored, and used by Defendants, and have not been
26 destroyed, and due to the continuing threat of such injury, have no adequate remedy at law,
27 entitling Plaintiffs to injunctive relief.

28
COUNT IV
VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT

CALIFORNIA PENAL CODE SECTION 630 *et seq.*

75. Plaintiffs reallege and incorporate the above allegations by reference as if set forth herein at length.

76. Plaintiffs assert this claim against Carrier IQ on behalf of themselves and the Class. Plaintiffs have standing to assert civil causes of action pursuant to California Penal Code § 637.2(a) which states “[a]ny person who has been injured by a violation of this chapter may bring an action against the person who committed the violation for greater of the following amounts: (1) Five thousand dollars (\$5,000); (2) Three times the amount of actual damages, if any, sustained by the plaintiff.”

77. California Penal Code section 630 provides, in part:

Any person who, . . . willfully and without the consent of all parties to the communication, or in any unauthorized manner, read, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passive over wire, line, or cable, or is being sent from , or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained or who aids, agrees with, employees, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable . . .

78. On information and belief, Plaintiffs, and each member of the Class, did not consent to any of the Defendants’ actions in intercepting, reading, and/or learning the contents of their communications.

79. The actions alleged herein were not undertaken “for the purpose of construction, maintenance, conduct or operation of the service and facilities of the public utility.”

80. Plaintiffs have additionally suffered loss by reason of these violations, including, without limitation, violation of the right to privacy. Defendant Carrier IQ asserts in its marketing materials that, with its software installed on a cellular device, a carrier can: “Identify exactly how your customers interact with services and which ones they use. See which content they consume, even offline.” But information about the

1 services consumers use is private. Information about the “content they consume” is
2 private. Consumers own this information, and Defendants have taken it without just
3 compensation. Plaintiffs and Class members seek to be given the monetary value of this
4 private data that was transmitted and sold.

5 81. Unless restrained and enjoined, Defendants will continue to commit such acts,
6 Pursuant to Sections 637.2 of the California Penal code, Plaintiffs have been injured and
7 are entitled to seek damages and injunctive relief.

8
9 COUNT V
10 VIOLATION OF THE UNFAIR COMPETITION LAW
11 CAL. BUS. & PROF. Code §§ 17200 *et seq.*

12 82. Plaintiffs reallege and incorporate the above allegations by reference as if set
13 forth herein at length.

14 83. California’s Unfair Competition Law (“UCL”) defines unfair competition to
15 include any “unlawful, unfair, or fraudulent” business act or practice.

16 84. Defendants engaged in “unlawful” business practices under the UCL because
17 they violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, the Electronic
18 Communications Privacy Act of 1986, 18 U.S.C. § 2510, the California Computer Crime
19 Law, California Penal Code § 502, and the California Invasion of Privacy Act, California
20 Penal Code § 630.

21 85. Defendants engaged in “fraudulent” business practices under the UCL
22 because they secretly installed the CIQ software on Plaintiffs’ devices, failed to disclose
23 that the CIQ software was always operating on such devices, failed to disclose that the
24 CIQ software was capable of intercepting Plaintiffs’ private communications and, in fact
25 intercepted such communications, and failed to disclose that the CIQ software degraded
26 the performance and battery life of the devices on which it was installed. Further,
27 Defendants surreptitiously took private and confidential information from Plaintiffs and
28 the other members of the Class. Defendants’ acts, omissions and failures to disclose were
“material” to Plaintiffs and the class within the meaning of *In re Tobacco II Cases*, 46 Cal.
4th 298 (Cal. 2009).

SECTION 1. All people are by nature free and independent and have inalienable rights. Amount these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.

88. Plaintiffs and the Class were injured in fact and lost money or property as a result of these unlawful, unfair, and fraudulent business practices. In particular and without limitation, Defendants have taken Plaintiffs' personal, private information for commercial purposes without their consent or agreement and otherwise without legal authority to do so. Further, Plaintiffs did not receive the performance level and battery life on their phones that they paid for because the CIQ software necessarily degraded such performance and battery life by constantly running on Plaintiffs' devices.

89. Plaintiffs reallege and incorporate the above allegations by reference as if set forth herein at length.

1 90. The Consumers Legal Remedies Act ("CLRA"), California Civil Code § 1750
2 *et seq*, applies to Defendants' actions and conduct because such actions and conduct
3 pertain to transactions that were intended to result and/or resulted in the sale of goods and
4 services to consumers.

5 91. Plaintiffs and each member of the Class are "consumers" within the meaning
6 of Civil Code § 1761(d).

7 92. The cellular devices that are the subject of this litigation are "goods" and
8 "services" within the meaning of Civil Code § 1761(a) and (b).

9 93. Defendants engaged in deceptive practices, unlawful methods of competition,
10 unfair acts, or any combination, as defined by Civil Code § 1770, to the detriment of
11 Plaintiffs and the Class. Plaintiffs and all other Class members have suffered and will
12 continue to suffer harm as a proximate result of the violations of law and wrongful conduct
13 of Defendants alleged herein.

14 94. Defendants used the following unfair or deceptive acts or practices in a
15 transaction intended to result in the sale of goods to Plaintiffs, as follows:

16 In violation of Civil Code § 1770(a)(7), Defendants represented that goods or
17 services are of a particular standard, quality, or grade, or that goods are of a
18 particular style or model, if they are of another.

19 In violation of Civil Code § 1770(a)(14), Defendants represented that a transaction
20 confers or involves rights, remedies, or obligations which it does not have or
21 involve, or which are prohibited by law.

22 95. In addition, Defendants concealed material information regarding the invasion
23 of private data and actions performed on cellular devices, as set forth herein. Defendants
24 concealed the presence of Carrier IQ's software on its customers' phones. The software
25 works in the background and degrades the operation of the phone and depletes the battery
26 unnecessarily. Thus, the quality of the phone was not properly characterized by
27 Defendants. Also, Defendants failed to inform consumers and the public that the
28 transaction involved the consumers' obligation to provide private data to carriers, which is
prohibited by law. Had Defendants disclosed this material information, Defendants could

1 not have charged Plaintiffs and Class members what they charged for their cellular
2 devices, and Carrier IQ could not have received the sums it did for transmission of data.

3 96. Defendants' acts and omissions and unfair business practices occurred in the
4 course of selling consumer products and violat Civil Code § 1770(a).

5 97. By this action, Plaintiffs and the Class seek injunctive relief and all other
6 relief that this Court deems just and proper.

7 PRAYER FOR RELIEF

8 WHEREFORE, Plaintiffs on behalf of themselves and all other similarly situated,
9 pray for judgment against Defendants as follows:

10 A. Certify this case as a class action on behalf of the Class as defined above,
11 appoint Plaintiffs as class representatives, and appoint Plaintiffs' counsel as class counsel.

12 B. Declare that the actions of Defendants, as set out above, violate the following:

- 13 i. Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et seq*;
14 ii. Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq*;
15 iii. California's Computer Crime Law, Penal Code § 502, *et seq*;
16 iv. California Invasion of Privacy Act, California Penal Code § 630, *et seq*;
17 v. California Unfair Business Practices Act §§ 17200, *et seq.*; and
18 vi. California Consumers Legal Remedies Act §§ 1750, *et seq.*

19 C. Award damages, including statutory damages where applicable, to Plaintiffs
20 and Class members in an amount to be determined at trial;

21 D. Award restitution against Defendants for all money to which Plaintiffs and the
22 Class are entitled in equity;

23 E. Restrain Defendants, their officers, agents servants, employees, and attorneys,
24 and those in active concert or participation with them form continued access, collection
25 and transmission of Plaintiffs' and Class members' personal information via preliminary
26 and permanent injunction;

27 F. Award Plaintiffs and the Class their reasonable litigation expenses, costs of
28 court, and attorneys' fees; and

1 G. All other and further relief as this Court may deem just and proper.

2 **ROSMAN & GERMAIN LLP**

3 

4 Dated: December 12, 2011

5 Daniel L. Germain (Bar No. 143334)
6 16311 Ventura Blvd., Suite 1200
7 Encino, CA 91436-2152
8 Telephone: (818) 788-0877
9 Facsimile: (818) 788-0885
E-Mail: R&G@Lalawyer.com

10 David M. Cialkowski
11 Brian C. Gudmundson
12 **ZIMMERMAN REED, P.L.L.P.**
13 1100 IDS Center
14 80 South 8th Street
15 Minneapolis, MN 55402
16 Telephone: (612) 341-0400
17 Facsimile: (612) 341-0844
18 E-Mail: David.Cialkowski@zimmreed.com

19 Timothy G. Blood (Bar No. 149434)
20 Paula M. Roach (Bar No. 254142)
21 **BLOOD HURST & O'REARDON, LLP**
22 600 B Street, Suite 1550
23 San Diego, CA 92101
24 Telephone: (619) 338-1100
25 Facsimile: (619) 338-1101
26 E-Mail: TBlood@bholaw.com

27 *Attorneys for Plaintiffs and the proposed*
28 *Class*

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury.

ROSMAN & GERMAIN LLP



Dated: December 12, 2011

Daniel L. Germain (Bar No. 143334)
16311 Ventura Blvd., Suite 1200
Encino, CA 91436-2152
Telephone: (818) 788-0877
Facsimile: (818) 788-0885
E-Mail: R&G@Lalawyer.com

David M. Cialkowski
Brian C. Gudmundson
ZIMMERMAN REED, P.L.L.P.
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
E-Mail: David.Cialkowski@zimmreed.com

Timothy G. Blood (Bar No. 149434)
Paula M. Roach (Bar No. 254142)
BLOOD HURST & O'REARDON, LLP
600 B Street, Suite 1550
San Diego, CA 92101
Telephone: (619) 338-1100
Facsimile: (619) 338-1101
E-Mail: TBlood@bholaw.com

*Attorneys for Plaintiffs and the proposed
Class*

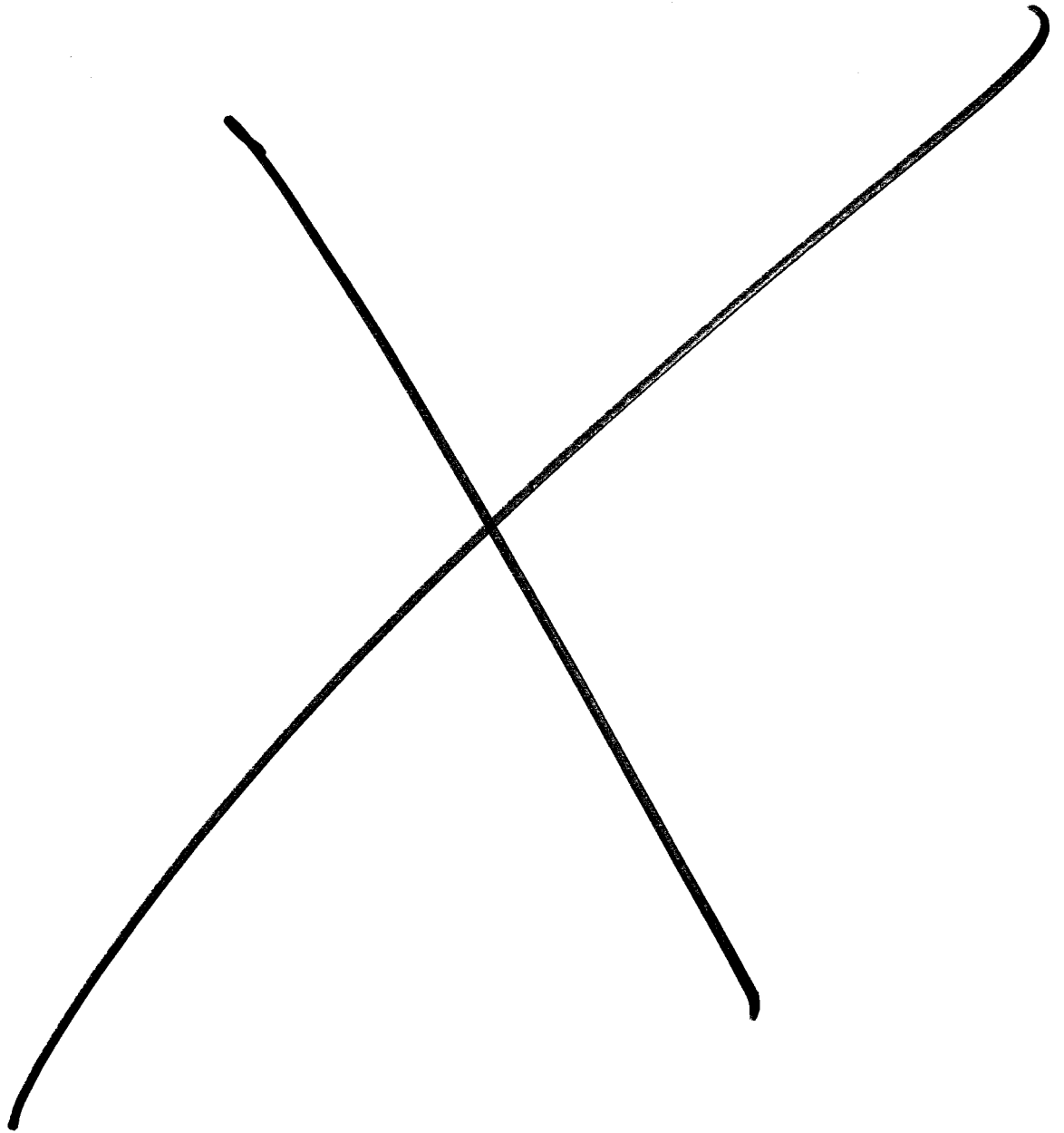


Exhibit 2:

Olivares, et al. v. Carrier IQ, Inc., et al.

**U.S. District Court
California Northern District (San Jose)
CIVIL DOCKET FOR CASE #: 5:11-cv-06151-HRL**

Olivares et al v. Carrier IQ, Inc et al
Assigned to: Magistrate Judge Howard R. Lloyd
Demand: \$5,000,000
Cause: 28:1331 Fed. Question

Date Filed: 12/06/2011
Jury Demand: Plaintiff
Nature of Suit: 890 Other Statutory
Actions
Jurisdiction: Federal Question

Plaintiff

Israel Olivares
*individuals, on behalf of themselves and
others similarly situated*

represented by **Brian R Strange**
Strange and Carpenter
12100 Wilshire Boulevard Suite 1900
Los Angeles, CA 90025
310-207-5055
Fax: 310-826-3210
Email: jacounsel@earthlink.net
ATTORNEY TO BE NOTICED

Joseph H Malley
Law Office of Joseph H. Malley, PC
1045 North Zang Boulevard
Dallas, TX 75208
214-943-6100
Email: malleylaw@gmail.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

Clarissa Portals
*individuals, on behalf of themselves and
others similarly situated*

represented by **Brian R Strange**
(See above for address)
ATTORNEY TO BE NOTICED

Joseph H Malley
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

Dao Phong

represented by **Mark Punzalan**
Finkelstein, Thompson LLP
100 Bush Street
Suite 1450
San Francisco, CA 94104
415-398-8700
Fax: 415-398-8704
Email: mpunzalan@finkelsteinthompson.com
ATTORNEY TO BE NOTICED

V.

Defendant

Carrier IQ, Inc
a Delaware corporation

Defendant

HTC America, Inc.
a Washington corporation

Date Filed	#	Docket Text
12/06/2011	<u>1</u>	Alleged Class Action Complaint (Summons Issued); jury demand; against Carrier IQ, Inc, HTC America, Inc. (Filing fee \$ 350, receipt number 54611010954). Filed by Clarissa Portals, Israel Olivares. (bw, COURT STAFF) (Filed on 12/6/2011) (Additional attachment(s) added on 12/12/2011: # <u>1</u> Civil Cover Sheet) (bw, COURT STAFF). (Entered: 12/08/2011)
12/06/2011	<u>2</u>	Summons Issued as to Carrier IQ, Inc, HTC America, Inc.. (bw, COURT STAFF) (Filed on 12/6/2011) (bw, COURT STAFF). (Entered: 12/08/2011)
12/06/2011	<u>3</u>	ADR SCHEDULING ORDER: Case Management Statement due by 2/28/2012. Case Management Conference set for 3/6/2012 01:30 PM in Courtroom 2, 5th Floor, San Jose. (bw, COURT STAFF) (Filed on 12/6/2011) (bw, COURT STAFF). (Entered: 12/08/2011)
12/06/2011		CASE DESIGNATED for Electronic Filing. (bw, COURT STAFF) (Filed on 12/6/2011) (Entered: 12/08/2011)
12/19/2011	<u>4</u>	Administrative Motion to Consider Whether Cases Should be Related (Kenny et al. v. Carrier IQ, Inc., et al. Case No. CV-11-5774-EJD Steiner v. Carrier IQ, Inc., Case No. CV-11-5802-EJD Silvera et al. v. Carrier IQ, Inc. et al., Case No. CV-11-5821-EJD Thomas et al. v. Carrier IQ, Inc. et al., Case No. CV-11-5819 LHK Pipkin et al. v. Carrier IQ, Inc. et al., Case No. CV-11-5820 EJD Patrick et al. v. Carrier IQ, Inc. et al., Case No. CV-11-5842-EJD Padilla et al. v. Carrier IQ, Inc. et al, Case No. CV-11-5975-EJD, Olivares et al. v. Carrier IQ, Inc. et al., Case No. CV-11-6151 HRL Stoltenburg et al. v. Carrier IQ, Inc. et al., ase No. CV-11-6160-PSG Medine et al. v. Carrier IQ, Inc. et al., Case No. CV-11-6178-HSG Fischer et al. v. Carrier IQ, Inc. et al., Case No. CV-11-6199-HRL Castro v. Carrier IQ, Inc. et al., Case No. CV-11-6201-PSG Gonzalez v. Carrier IQ, Inc. et al., Case No. CV-11-6202-HRL House v. Carrier IQ, Inc. et al., Case No. CV-11-6200-LHK Lavertue v. Carrier IQ, Inc. et al., Case No. CV-11-6196-MEJ Shumate v. Carrier IQ, Inc., Case No. CV-11-6281-HRL, Wadler v. Carrier IQ, Inc., Case No. CV-11-6278-PSG, Schwartz v. Carrier IQ, Inc., Case No. CV-11- 6280-HRL, Massey v. Carrier IQ, Inc. Case No. CV-11-6279-HRL) filed by Dao Phong. (Attachments: # <u>1</u> Declaration, # <u>2</u> Exhibit, # <u>3</u> Exhibit, # <u>4</u> Exhibit, # <u>5</u> Exhibit, # <u>6</u> Exhibit, # <u>7</u> Exhibit, # <u>8</u> Exhibit, # <u>9</u> Exhibit, # <u>10</u> Exhibit, # <u>11</u> Exhibit, # <u>12</u> Exhibit, # <u>13</u> Exhibit, # <u>14</u> Exhibit, # <u>15</u> Exhibit, # <u>16</u> Exhibit, # <u>17</u> Exhibit, # <u>18</u> Exhibit, # <u>19</u> Exhibit, # <u>20</u> Exhibit, # <u>21</u> Exhibit, # <u>22</u> Certificate/Proof of Service) (Punzalan, Mark) (Filed on 12/19/2011) Modified on 12/20/2011 (bw, COURT STAFF). (Entered: 12/19/2011)

1 STRANGE & CARPENTER
2 Brain R. Strange (Cal. Bar. No. 103252)
3 LACounsel@earthlink.net
4 12100 Wilshire Boulevard, Suite 1900
5 Los Angeles, CA 90025
6 Telephone: (310) 207-5055
7 Facsimile: (310) 826-3210

8 LAW OFFICE OF JOSEPH MALLEY
9 Joseph H. Malley (*pro hac vice* pending)
10 malleylaw@gmail.com
11 1045 North Zang Blvd
12 Dallas, TX 75208
13 Telephone: (214) 943-6100

14 Attorneys for Plaintiffs

15 IN THE UNITED STATES DISTRICT COURT
16 FOR THE NORTHERN DISTRICT OF CALIFORNIA
17 SAN JOSE DIVISION

18 ISRAEL OLIVARES; CLARISSA PORTALES;
19 individuals, on behalf of themselves and others
20 similarly situated,

21 Plaintiffs,

22 v.

23 CARRIER IQ, INC., a Delaware Corporation;
24 HTC AMERICA, INC., a Washington
25 corporation;

26 Defendant.

27 CASE No.

28 DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT FOR
VIOLATIONS OF:

1. ELECTRONIC COMMUNICATIONS
PRIVACY ACT, 18 U.S.C. §2510;
2. STORED COMMUNICATIONS ACT,
18 U.S.C. §2701;
3. CONSUMER LEGAL REMEDIES
ACT, ("CLRA") CALIFORNIA CIVIL
CODE § 1750;
4. UNFAIR COMPETITION LAW,
CALIFORNIA BUSINESS AND
PROFESSIONS CODE §17200;
5. CALIFORNIA'S COMPUTER CRIME
LAW, PENAL CODE §502;
6. CALIFORNIA INVASION OF
PRIVACY ACT, PENAL CODE §630;
7. SONG-BEVERLY WARRANTY ACT,
CALIFORNIA CIVIL CODE § 1792
8. TEXAS DECEPTIVE TRADE
PRACTICES ACT, TEXAS

CLASS ACTION COMPLAINT

ORIGINAL FILED

DEC - 6 2011

Richard W. Wiaking
Clerk, U.S. District Court
Northern District of California
San Jose

E-filing

ADR

By fap

CV11-06151

HRL

BUSINESS AND COMMERCE CODE
§ 17.41
9. BREACH OF EXPRESS WARRANTY
10. BREACH OF IMPLIED WARRANTY
11. NEGLIGENCE
12. TRESPASS TO PERSONAL
PROPERTY/ CHATTELS
13. CONVERSION
14. UNJUST ENRICHMENT

1. Plaintiffs, Israel Olivares, and Clarissa Portales, (collectively, "Plaintiffs"), by and through their attorneys Strange & Carpenter, and Law Office of Joseph H. Malley, P.C., bring this action on behalf of themselves and all others similarly situated, against Carrier IQ, Inc. ("Carrier IQ") and HTC, America, Inc. ("HTC"), (collectively with Carrier IQ, "Defendants"). Plaintiffs' allegations as to themselves and their own actions, as set forth herein, are based upon their information and belief and personal knowledge. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. §1332(d) as set forth below.

I. NATURE OF THE ACTION

2. Plaintiffs bring this consumer Class Action lawsuit pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3) on behalf of themselves and a proposed class of similarly situated consumers ("Class Members") who purchased an HTC mobile device on which Carrier IQ's software, "HTC IQAgent," was installed, without notice or consent of Plaintiffs. This HTC IQAgent software was designed by Carrier IQ and customized by HTC in order to log and collect confidential, unencrypted user data including but not limited to (1) the contents of incoming text messages; (2) the URLs of websites visited by the user; and (3) the user's GPS coordinates; among other private and personally-identifying data. HTC IQAgent records this confidential data on a user's mobile device in an unencrypted format so that any device software or applications with log file permission can access and review it. Carrier IQ and HTC also have access to this confidential data and can transmit the data from a user's mobile device to remote servers at any time via hidden "text requests" sent to a user's mobile device by Carrier IQ, HTC or other authorized third parties. HTC IQAgent logs the hidden text

CLASS ACTION COMPLAINT

1 requests and the confidential data silently so that a user has no idea that data is being collected
2 and transmitted. HTC IQAgent is preinstalled on HTC's mobile devices so that data logging
3 begins the moment a user purchases and turns on the device, without notice to or consent from
4 the user. Because the software is preinstalled by HTC and runs as part of the device operating
5 system, data is automatically collected and can be transmitted via wireless internet or other
6 means, even if the device user has no carrier contract and the mobile device is not connected to
7 a mobile network. Finally, HTC IQAgent runs continuously and depletes resources on the
8 mobile device without notice to or authorization of the user, even when the mobile device is
9 not being used. The resources depleted by HTC IQAgent without notice or authorization
10 include (1) battery power; (2) device memory; (3) CPU; (4) bandwidth; and (5) text messages.
11 A user cannot stop the HTC IQAgent software from running under any circumstances, and a
12 user is unable to remove HTC IQAgent from the device without voiding the manufacturer's
13 warranty.

14 3. Because of Defendants' actions, Plaintiffs and Class Members are victims of
15 unfair, deceptive, and unlawful business practices; wherein their privacy, financial interests,
16 and security rights, were violated by Carrier IQ and HTC. Plaintiffs and Class Members were
17 financially harmed by the Defendants when they purchased the HTC mobile devices with HTC
18 IQAgent, and Plaintiffs would not have purchased those devices if they had known that
19 Defendants' software could access, collect, transmit, analyze, store, and provide their
20 confidential unencrypted data to any device software or applications with log file permission
21 without Plaintiffs' knowledge of permission. Plaintiffs and Class Members were also harmed
22 by HTC and Carrier IQ's unauthorized use of their mobile device battery power, device
23 memory, CPU, bandwidth and text messages.

24 4. HTC manufactured and sold to Plaintiffs and Class Members without notice, a
25 defective product that included HTC IQAgent, specially customized by HTC for use on its
26 mobile device. HTC acted individually, and in concert with, Carrier IQ to gain unauthorized
27 access to, log, collect, and transmit Plaintiffs' and Class Members' confidential, unencrypted
28 data and to provide third-party access to this data. HTC IQAgent is a native HTC application

1 that was installed on HTC mobile devices with the knowledge of HTC.

2 5. Carrier IQ acted independently, and in concert with HTC, knowingly
3 authorizing, directing, ratifying, acquiescing in, or participating in the conduct alleged herein.

4 6. Carrier IQ individually, and in concert with HTC has been systematically
5 engaged in and facilitated a covert operation of logging and tracking Plaintiffs' and Class
6 Members' confidential, unencrypted user data and utilizing Plaintiffs' and Class Members'
7 mobile device resources, violating one or more of the following:

8 (a) ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C.
9 §2510;

10 (b) STORED COMMUNICATIONS ACT, 18 U.S.C. §2701;

11 (c) CONSUMER LEGAL REMEDIES ACT, ("CLRA") CALIFORNIA
12 CIVIL CODE § 1750;

13 (d) UNFAIR COMPETITION LAW, CALIFORNIA BUSINESS AND
14 PROFESSIONS CODE §17200;

15 (e) CALIFORNIA'S COMPUTER CRIME LAW, PENAL CODE §502;

16 (f) CALIFORNIA INVASION OF PRIVACY ACT, PENAL CODE
17 §630;

18 (g) SONG-BEVERLY WARRANTY ACT, CALIFORNIA CIVIL CODE
19 § 1792

20 (h) TEXAS DECEPTIVE TRADE PRACTICES ACT, TEXAS
21 BUSINESS AND COMMERCE CODE § 17.41

22 (i) BREACH OF EXPRESS WARRANTY

23 (j) BREACH OF IMPLIED WARRANTY

24 (k) NEGLIGENCE

25 (l) TRESPASS TO PERSONAL PROPERTY/ CHATTELS

26 (m) CONVERSION

27 (n) UNJUST ENRICHMENT

28 **II. JURISDICTION AND VENUE**

1 7. This Court has subject matter jurisdiction pursuant to the Class Action Fairness
2 Act of 2005, 28 U.S.C. § 1332(d), because at least one class member is of diverse citizenship
3 from Defendants; there are more than 100th class members nationwide; and the aggregate
4 amount in controversy exceeds \$5,000,000 and minimal diversity exists.

5 8. Venue is proper in this District under 28 U.S.C. §1391(b) and (c) against
6 Defendants. A substantial portion of the events, conduct and omissions giving rise to the
7 violations of law complained of herein occurred in this District. Carrier IQ's principal
8 executive offices and headquarters are located in this District at 1200 Villa Street, Suite 200,
9 Mountain View, CA 94041.

10 9. This Court has personal jurisdiction over the Defendants because Carrier IQ
11 maintains its corporate headquarters in, and the events, conduct and omissions giving rise to
12 the violations of law complained herein occurred in California. HTC conducts business in
13 California and engaged in the acts alleged herein in California.

14 10. This Court also has subject matter jurisdiction over all causes of action and the
15 Defendants implicated therein pursuant to 28 U.S.C. §1332(d), and because this action arises in
16 part under a federal statute and this Court has jurisdiction pursuant to 18 U.S.C. §2710(c)
17 which confers jurisdiction in the United States District Court for actions related to the
18 Electronic Communications Privacy Act 18 U.S.C. §2510 and the Stored Communications Act,
19 18 U.S.C. §2701.
20

21 11. **INTRADISTRICT ASSIGNMENT:** Pursuant to Civil Local Rule 3-2(e), this
22 case shall be assigned to the San Jose Division as it arises from Santa Clara County where
23 Defendant Carrier IQ is headquartered and where the actions alleged as the basis of this claim
24 took place.

25 **III. PARTIES**

26 12. Plaintiff Israel Olivares ("Olivares") is a citizen and resident of California, (San
27 Diego County, California). On information and belief, Olivares incorporates all allegations
28 within this complaint. Olivares is a representative of the class ("Class"), as defined within the
Class Allegations. In or around February 2011, Olivares purchased an HTC EVO 4G mobile

1 device that was preinstalled with HTC IQAgent, and used such mobile device on one or more
2 occasions during the class period in California.

3 13. Olivares was not aware that HTC IQAgent was installed on his HTC device,
4 and was not aware that every time he used his HTC device, HTC IQAgent was logging and
5 collecting his confidential incoming text messages; the URLs of websites he visited; and his
6 actual GPS coordinates; among other private and personally-identifying data. He also was not
7 aware that HTC IQAgent made this confidential, unencrypted data available on Olivares's
8 mobile device log so that any device software or applications with log file permission could
9 access it. Finally, Olivares was not aware that HTC IQAgent depleted his mobile device
10 battery power, device memory, CPU, bandwidth and text messages, even while he was not
11 using his device. The HTC IQAgent software does not show up under the application launch
12 list on Olivares's device.

13 14. Plaintiff Clarissa Portales ("Portales") is a citizen and resident of Dallas, Texas,
14 (Dallas County, Texas). On information and belief, Portales incorporates all allegations within
15 this complaint. Portales is a representative of the Class, as defined within the Class Allegations.
16

17 On January 2011, Portales purchased a an HTC EVO 4G mobile device that was preinstalled
18 with HTC IQAgent, and used such mobile device, on one or more occasions during the class
19 period in Texas.

20 15. Portales was not aware that HTC IQAgent was installed on her HTC device, and
21 was not aware that every time she used her HTC device, HTC IQAgent was logging and
22 collecting her confidential incoming text messages; the URLs of websites she visited; and her
23 actual GPS coordinates; among other private and personally-identifying data. She also was not
24 aware that HTC IQAgent made this confidential, unencrypted data available on Portales's
25 mobile device log so that any device software or applications with log file permission could
26 access it. Finally, Portales was not aware that HTC IQAgent depleted her mobile device battery
27 power, device memory, CPU, bandwidth and text messages, even while she was not using her
28 device. The HTC IQAgent software does not show up under the application launch list on
Portales's device.

1 16. Carrier IQ is a Delaware corporation that maintains and has maintained at all
2 relevant times its headquarters at 1200 Villa Street, Suite 200, Mountain View, CA, 94041
3 (Santa Clara County, California). Carrier IQ does business throughout the United States, and in
4 particular, does business in the State of California and in this County.

5 17. HTC is a Washington corporation that maintains and has maintained at all
6 relevant times its headquarters at 13920 SE Eastgate Way, Bellevue, Washington 98005. HTC
7 does business throughout the United States, and in particular, does business in the State of
8 California and in this County.

9 **IV. PLAINTIFFS' EXPERIENCE**

10 18. At all relevant times herein, Plaintiffs were and are residents of California and
11 Texas. During the class period, Plaintiffs owned and operated one or more HTC mobile
12 devices installed with HTC IQAgent without Plaintiffs' knowledge.

13 19. On one or more occasions during the class period, Plaintiffs accessed and used
14 their HTC mobile devices to receive text messages and visit websites in their cities of residence
15 and elsewhere.

16 20. During the relevant class period, the HTC IQAgent software was "hidden" and
17 did not appear on application launch menu on Plaintiffs' HTC mobile devices. During the
18 relevant class period, Plaintiffs were unaware that HTC IQAgent populated and logged
19 incoming text messages, visited URLs and GPS location data on their device log files.
20 Plaintiffs were also unaware that this confidential data was available, unencrypted, to all
21 software and programs with log file permission running on their devices. Additionally, they
22 were unaware that HTC IQAgent had the mechanisms to, and did, transmit user data from
23 Plaintiffs' devices to remote servers via periodic scheduling, WAP push requests, and text
24 requests.
25

26 21. During the relevant class period, HTC IQAgent, customized in part by HTC,
27 was "hidden" and did not appear on the launch list of applications and software installed on
28 Plaintiffs' HTC mobile devices.

22. In or around November 2011, Plaintiffs became aware of information related to

the tracking activities of Carrier IQ and HTC. Plaintiffs downloaded a "log collector" application to determine whether their mobile device possessed the Carrier IQ software. The log collector is an application that collects a device log identifying software and applications are running on a mobile device. Plaintiffs then accessed their HTC mobile device and engaged in basic user activity such as doing websearches, accessing their Facebook accounts, updating their Facebook "status," calling friends, sending text messages, and downloading applications.

23. Olivares's log revealed the data collection and transmission actions of Carrier IQ within his HTC mobile device which existed without notice or authorization, (highlighting added):

11-21 13:10:03.692 V/AgentService_J(237):
Action[1026]:com.htc.android.iqagent.action.ui08
11-21 13:10:10.168 V/AgentService_J(237):
Action[1027]:com.htc.android.iqagent.action.ui19
11-21 13:10:10.358 V/AgentService_J(237):
Action[1028]:com.htc.android.iqagent.action.ui19
11-21 13:10:15.463 V/AgentService_J(237):
Action[1029]:com.htc.android.iqagent.action.ui19
11-21 13:10:16.304 V/AgentService_J(237):
Action[1030]:com.htc.android.iqagent.action.ui19
11-21 13:10:18.566 V/AgentService_J(237):
Action[1031]:com.htc.android.iqagent.action.ui19
11-21 13:10:18.596 V/AgentService_J(237):
Action[1032]:com.htc.android.iqagent.action.ui19
11-21 13:10:19.397 V/AgentService_J(237):
Action[1033]:com.htc.android.iqagent.action.ui08
11-21 13:10:28.336 V/AgentService_J(237):
Action[1034]:com.htc.android.iqagent.action.ui08
11-21 13:10:30.628 V/AgentService_J(237):
Action[1035]:com.htc.android.iqagent.action.ui08
11-21 13:10:32.820 V/AgentService_J(237):
Action[1036]:com.htc.android.iqagent.action.ui08
11-21 13:10:35.062 V/AgentService_J(237):
Action[1037]:com.htc.android.iqagent.action.ui08
11-21 13:10:35.072 V/AgentService_J(237):
Action[1038]:com.htc.android.iqagent.action.ui08
11-21 13:10:44.011 V/AgentService_J(237):
Action[1039]:com.htc.android.iqagent.action.ui08
11-21 13:10:46.263 V/AgentService_J(237):
Action[1040]:com.htc.android.iqagent.action.ui08
11-21 13:10:48.505 V/AgentService_J(237):
Action[1041]:com.htc.android.iqagent.action.ui08
11-21 13:10:50.737 V/AgentService_J(237):

1 Action[1042]:com.htc.android.iqagent.action.ui08
11-21 13:10:52.960 V/AgentService_J(237):
2 Action[1043]:com.htc.android.iqagent.action.ui15
11-21 13:10:52.970 V/AgentService_J(237):
3 Action[1044]:com.htc.android.iqagent.action.ui08
11-21 13:10:53.060 V/AgentService_J(237):
4 Action[1045]:com.htc.android.iqagent.action.ui15
11-21 13:10:58.415 V/AgentService_J(237):
5 Action[1046]:com.htc.android.iqagent.action.ui08
11-21 13:10:59.616 V/AgentService_J(237):
6 Action[1047]:com.htc.android.iqagent.action.ui08
11-21 13:11:04.211 V/AgentService_J(237):
7 Action[1048]:com.htc.android.iqagent.action.ui08
11-21 13:11:12.959 V/AgentService_J(237):
8 Action[1049]:com.htc.android.iqagent.action.ui13
11-21 13:11:13.480 V/AgentService_J(237):
9 Action[1050]:com.htc.android.iqagent.action.ui13
11-21 13:11:21.547 V/AgentService_J(237):
10 Action[1051]:com.htc.android.iqagent.action.ui19
11-21 13:11:21.598 V/AgentService_J(237):
11 Action[1052]:com.htc.android.iqagent.action.ui13
11-21 13:11:22.278 V/AgentService_J(237):
12 Action[1053]:com.htc.android.iqagent.action.ui08
11-21 13:11:22.288 V/AgentService_J(237):
13 Action[1054]:com.htc.android.iqagent.action.ui19
11-21 13:11:22.829 V/AgentService_J(237):
14 Action[1055]:com.htc.android.iqagent.action.ui15
11-21 13:11:24.340 V/AgentService_J(237):
15 Action[1056]:com.htc.android.iqagent.action.ui08

16
17
18
19 24. Portales's log revealed the data collection and transmission actions of Carrier IQ
20 within her HTC mobile device which existed without notice or authorization, (highlighting
21 added):

22 11-21 12:03:47.039 V/AgentService_J(16252):
23 Action[441]:com.htc.android.iqagent.action.ui15
11-21 12:03:47.069 V/AgentService_J(16252):
24 Action[442]:com.htc.android.iqagent.action.ui02
11-21 12:03:47.079 V/AgentService_J(16252):
25 Action[443]:com.htc.android.iqagent.action.ui15
11-21 12:03:47.079 V/AgentService_J(16252):
26 Action[444]:com.htc.android.iqagent.action.ui15
11-21 12:03:47.079 V/AgentService_J(16252):
27 Action[445]:com.htc.android.iqagent.action.ui15
11-21 12:03:47.079 V/AgentService_J(16252):
28 Action[446]:com.htc.android.iqagent.action.ui19
11-21 12:03:47.220 V/AgentService_J(16252):

CLASS ACTION COMPLAINT

1 Action[447]:com.htc.android.iqagent.action.ui08
11-21 12:03:49.222 V/AgentService_J(16252):
2 Action[448]:com.htc.android.iqagent.action.ui08
11-21 12:03:50.032 V/AgentService_J(16252):
3 Action[449]:com.htc.android.iqagent.action.ui13
11-21 12:03:50.243 V/AgentService_J(16252):
4 Action[450]:com.htc.android.iqagent.action.ui15
11-21 12:03:50.993 V/AgentService_J(16252):
5 Action[451]:com.htc.android.iqagent.action.ui19
11-21 12:03:51.424 V/AgentService_J(16252):
6 Action[452]:com.htc.android.iqagent.action.ui19
11-21 12:03:51.454 V/AgentService_J(16252):
7 Action[453]:com.htc.android.iqagent.action.ui08
11-21 12:03:53.706 V/AgentService_J(16252):
8 Action[454]:com.htc.android.iqagent.action.ui08
11-21 12:03:55.948 V/AgentService_J(16252):
9 Action[455]:com.htc.android.iqagent.action.ui08
11-21 12:04:02.665 V/AgentService_J(16252):
10 Action[456]:com.htc.android.iqagent.action.ui08
11-21 12:04:06.418 V/AgentService_J(16252):
11 Action[457]:com.htc.android.iqagent.action.ui19
11-21 12:04:06.428 V/AgentService_J(16252):
12 Action[458]:com.htc.android.iqagent.action.ui13
11-21 12:04:06.488 V/AgentService_J(16252):
13 Action[459]:com.htc.android.iqagent.action.ui15
11-21 12:04:06.659 V/AgentService_J(16252):
14 Action[460]:com.htc.android.iqagent.action.ui19
11-21 2:04:09.401 V/AgentService_J(16252):
15 Action[461]:com.htc.android.iqagent.action.ui08
16

19 25. Plaintiffs consider information about their received text messages, visited
20 websites and GPS location to be in the nature of confidential and personal information that
21 they protect from disclosure, including by controlling their mobile device's privacy settings for
22 acceptance or rejection. Plaintiffs were not made aware by Defendants of the existence of HTC
23 IQAgent on their mobile devices or the logging, collection and transmission of their mobile
24 device data.

25 26. Plaintiffs also consider their device battery power, device memory, CPU,
26 bandwidth and text messages to be valuable personal property that they protect from
27 unauthorized use by third parties, including by controlling what software and applications have
28 access to those resources. Plaintiffs were not made aware by Defendants of the existence of

1 HTC IQAgent on their mobile devices or the depletion of their device battery power, device
2 memory, CPU, bandwidth and text messages by that software.

3 27. It is Plaintiffs' belief that The Carrier IQ software, customized in part by HTC,
4 was logging, collection and transmission of confidential user data on their mobile devices
5 permitted one or more objects within their mobile devices to be used for tracking and analysis
6 by Defendants and/or third parties, thus their mobile device data was obtained in an effort to
7 monitor and profile their mobile device activities. Plaintiffs did not receive notice of the
8 installation of a tracking identifier, did not consent to its installation, and did not want a
9 tracking identifier to be installed on their mobile device. Moreover, Plaintiffs did not authorize
10 Defendants to log, collect, transmit, or store their confidential mobile device data without
11 notice or express consent. Such software was running on Plaintiffs mobile device and
12 collecting and transmitting Plaintiffs data without notice or authorization, utilizing Plaintiffs
13 battery power, device memory, CPU, bandwidth, and limited text messages without notice or
14 authorization, even when Plaintiffs stopped actively using the device.

15 28. In selecting the HTC mobile device over the service and goods of other
16 competing mobile device manufacturers, Plaintiffs reasonably expected that their confidential
17 user data would not be accessed, logged and transmitted to third parties without their
18 knowledge and consent. They also reasonably expected that their mobile device resources
19 would not be depleted without their knowledge or control.

20 29. Had Plaintiffs known that the HTC devices they purchased would include
21 software that provided third party access to their confidential user data and their mobile device
22 resources without notice to or authorization by Plaintiffs, Plaintiffs would have not purchased
23 those devices.

24 30. Plaintiffs were harmed by Defendants' practices, including but not limited to the
25 following:

- 26 (a) Costs to purchase the defective HTC mobile device;
27 (b) Violations of Plaintiffs' legally protected federal, state and common
28 law rights of privacy, especially related to unencrypted logging, storage and transmission of

1 Plaintiffs' confidential user data;

2 (c) Time and expense to remedy the effects of Defendants' actions;

3 (d) Time and expense to repair Plaintiffs' mobile devices and remedy the
4 impaired operability caused by the Defendants;

5 (e) Loss of property due to the inability to re-sell Plaintiffs' and Class
6 Members' mobile devices due to the Carrier IQ application; and

7 (f) Financial harm by the Defendants' unauthorized use of Plaintiffs' and
8 mobile device resources during the unauthorized process of logging and transmitting user
9 data.

10 31. It is Plaintiffs' belief that HTC IQAgent's logging, collection and transmission
11 of confidential user data on their mobile devices permitted one or more objects within their
12 mobile devices to be used for tracking and analysis by Defendants and/or third parties, thus
13 their mobile device data was obtained in an effort to monitor and profile their mobile device
14 activities. Plaintiffs did not receive notice of the installation of a tracking identifier, did not
15 consent to its installation, and did not want a tracking identifier to be installed on their mobile
16 device. Moreover, Plaintiffs did not authorize Defendants to log, collect, transmit, or store their
17 confidential mobile device data without notice or express consent.

18 32. Defendants' business practices unfairly wrested from Plaintiffs control over
19 their user data privacy and control over their device resources. Defendants' logging, collection
20 and unencrypted disclosure of Plaintiffs' confidential user data violates user expectations,
21 diminishes user privacy, and contradicts the Manufacturer's Warranty. Defendants caused
22 harm and damages to Plaintiffs' finite device resources, thus preventing Plaintiffs to use the
23 devices for their intended purposes and resulting in instability issues.

24 **V. COMMON EXPERIENCES BETWEEN PLAINTIFFS AND CLASS MEMBERS**

25 33. At all relevant times herein, the sequence of events, and consequences common
26 to Plaintiffs and Class Members, made the basis of this action, include, but are not limited to
27 the following:
28

(a) Plaintiffs and Class Members are individuals in the United States who

1 purchased and used an HTC mobile device that had HTC IQAgent software installed and
2 customized by HTC, without notice or consent;

3 (b) HTC a mobile device manufacturer had entered into a legally binding
4 contract with Carrier IQ to host the HTC IQAgent software on its mobile device.

5 (c) Carrier IQ was aware that HTC had preinstalled HTC IQAgent on
6 Plaintiffs' and Class Members' mobile devices, aware. That HTC had customized y HTC
7 IQAgent, aware that HTC IQAgent was "hidden" and did not appear in the launch list of
8 applications installed on Plaintiffs' and Class Members' mobile devices;

9 (d) Plaintiffs and Class Members accessed and used their HTC mobile
10 devices that had the preinstalled or uploaded HTC IQAgent software application;

11 (e) Carrier IQ collected confidential user data from Plaintiffs' and Class
12 Members' mobile devices without the consent of, or notice to, Plaintiffs and Class Members;

13 (f) Carrier IQ sent Plaintiffs' and Class Members' unencrypted
14 confidential mobile device data to its servers located in California without notice to or
15 authorization from Plaintiffs and Class Members;

16 (g) HTC transmitted, and/or allowed access to Plaintiffs' and Class
17 Members' confidential mobile device data, without notice or authorization, to HTC and any
18 software with log file access on Plaintiffs' and Class Members' devices. Upon information
19 and belief, this confidential data was unencrypted when stored in the log file and during at
20 least some part of its transmission;

21 (h) Carrier IQ created a database related to Plaintiffs' and Class Members'
22 mobile device data and activities, to assist the Defendant's tracking scheme. Such tracking
23 could not be detected, managed or deleted, and provided, in whole or part, the collective
24 mechanism to track Plaintiffs and Class Members, without notice or consent;

25 (i) Carrier IQ conducted systematic and continuous surveillance of the
26 Plaintiffs' and Class Members' mobile device activity from its headquarters in California
27 which continues to date;

28 (j) Carrier IQ copied, used, and stored Plaintiffs' and Class Members'

1 mobile device data in California after it knowingly accessed, without authorization,
2 Plaintiffs' and Class Members' mobile devices;

3 (k) Carrier IQ obtained and retained the data in California for a period that
4 far exceeded the purpose claimed by Carrier IQ for obtaining the data;

5 (l) Carrier IQ obtained individually, and in concert with HTC, Plaintiffs'
6 and Class Members' confidential user data, derived, in whole or part, from its monitoring the
7 mobile device activities of Plaintiffs and Class Members. This sensitive information includes
8 but is not limited to incoming text messages, visited URLs and GPS coordinates;

9 (m) HTC and Carrier IQ failed to notify and warn Plaintiffs and Class
10 Members of Carrier IQ's logging and tracking activities involving their mobile devices
11 before, during, or after the unauthorized practices so that Plaintiffs and Class Members were
12 unable to take appropriate actions to opt-out of the unauthorized surveillance by Defendants
13 and other third parties;

14 (n) HTC failed to block access to, and void the licensing agreements of
15 Carrier IQ after it received notice of Carrier IQ's tracking actions made the basis of this
16 action;

17 (o) Carrier IQ and HTC failed to provide any terms of service or privacy
18 policy related to the use of HTC IQAgent for tracking Plaintiffs' and Class Members' mobile
19 activities, or provide an updated privacy policy or any notice alerting users of its activity,
20 made the basis of this action so that Plaintiffs and Class Members had no notice of such
21 activities, nor the ability to mitigate their harm and damage after the fact;

22 (p) Defendants converted Plaintiffs' and Class Members' mobile device
23 data, including but not limited to their incoming text messages, visited URLs and GPS
24 coordinates;

25 (q) Defendants depleted Plaintiffs' and Class Members' mobile device
26 resources while running the HTC IQAgent software, including the device battery power,
27 device memory, CPU, bandwidth and text messages.
28

34. Plaintiffs and Class Members involved with the Defendants were harmed by

Defendants' practices, including but not limited to the following:

(a) Violations of Plaintiffs' legally protected federal, state and common law rights of commerce and privacy, especially related to unencrypted transmission of Plaintiffs and Class Members' confidential and sensitive user data;

(b) Financial Harm due to the costs to purchase the defective HTC mobile device;

(c) Financial Harm due to the time and expense to remedy the effects of Defendants' actions;

(d) Financial Harm due to the time and expense to repair Plaintiffs' mobile devices and remedy the impaired operability caused by the Defendants;

(e) Financial Harm due to the loss of property due to the inability to re-sell Plaintiffs' and Class Members' mobile devices due to the Carrier IQ application;

(f) Financial Harm due to the loss of property due to the unauthorized access and use of Plaintiffs' and Class Members' confidential user data, depriving Plaintiffs and Class Members of such possession and use;

(g) Financial Harm due to the Defendants' unauthorized use of Plaintiffs' and Class Member's mobile device's battery power, device memory, CPU, bandwidth and text messages during the unauthorized process of obtaining user data;

VI. FACTUAL ALLEGATIONS

A. Background

35. On October 26, 1999 the Wireless Communication and Public Act of 1999 was enacted and became known as the "e911 Act." It was an amendment to the Telecommunication Act of 1996. The purpose of the bill was to promote and enhance public safety through the use of 911 as universal assistance number. The Federal Law mandated that mobile phones be embedded with a Global Positioning System ("GPS") chip, which could calculate a user's coordinates to within a few yards by receiving signals from satellites. This law enacted to aid those in harm's way, resulted in the computing industry developing hardware and software to assist in the development of this technology or mobile devices provided Carrier IQ the impetus

1 to originate a business plan to take advantage of the benefit of embedded GPS chips in all
2 mobile phones for its own commercial benefit:

3 This confluence of circumstances and events— rapid adoption of new
4 wireless technologies, improved resiliency of service, increased data
5 transmission rates, the e911 law requiring homing chips, and market
6 precedents which show that mobile device users are willing to pay for
7 wireless services or applications—establish the feature-rich wireless
8 station as an increasingly logical and compelling channel for the free
9 flow of communications, information, entertainment and commerce.

10 United States Patent No.: US 7,609,650 B2, COLLECTION OF DATA AT TARGET

11 WIRELESS DEVICES USING DATA COLLECTION PROFILES, Assignee: Carrier IQ, Inc.,

12 Mountain View, CA (US), Filed: July 5, 2005.

13 36. Carrier IQ's software is reportedly installed in excess of one hundred and fifty
14 million (150,000,000) mobile devices, including mobile devices manufactured by HTC. These
15 devices installed with HTC IQAgent inherently defective, and Defendants falsely advertised,
16 marketed and distributing these mobile devices, without disclosure of the material facts about
17 the defect, misrepresenting the performance of the devices, violating express and implied

18 warranties, thus rendering the mobile devices unable to be used for their intended purposes.
19 Such activities resulted in a pattern of covert mobile device surveillance, wherein Defendants
20 installed HTC IQAgent on Plaintiffs' and Class Members' mobile device without authorization
21 and consent, thereby committing unauthorized access, collection, storage, and use of, the
22 mobile device and data derived from the Plaintiffs' and Class Members' use of the mobile
23 devices and transmitting information, code, and commands to collect, monitor, and remotely
24 store non-anonymized Plaintiffs' and Class Members' confidential mobile device data.
25 Defendants unauthorized access of this confidential, unencrypted data also allowed access to
26 all software and applications with log file access so that Plaintiffs' and Class Members' data
27 could be transmitted by multiple unknown parties at any time, *like a pac-man creeping 150*
28 *million mobile phones and "calling home."*

37. The HTC-version of the software, HTC IQAgent, is currently preinstalled by
HTC on its Carrier IQ-enabled mobile devices and was also installed via software updates on

1 older HTC devices.

2 **B. Carrier IQ: "See What Content They Consume Even Offline"**

3 38. According to Carrier IQ, the software is designed to monitor, manage and
4 support mobile devices deployed across mobile operators, service providers and enterprises.
5 Carrier IQ's website explains:

6 [HTC IQAgent] provides a level of visibility into true customer
7 experience that was, previously unavailable in the mobile industry.
8 [HTC IQAgent] uses data directly from the mobile phone itself to give a
9 precise view of how users interact with both their phones and the
services delivered through them, even if the phone is not communicating
with the network.

10 <http://www.carrieriq.com/overview/IQInsightExperienceManager/index.htm> (last visited
11 December 5, 2011).

12 39. HTC IQAgent is a monitoring software that runs continuously in the
13 background reportedly to monitor device and application performance. When a particular event
14 or error associated with the device occurs, the software collects data associated with the event
15 or error and may upload it either in real time or at a later time to its data repository for analysis.

16 40. During the use of a mobile device in a mobile communication network,
17 parameter data defining conductors associated with the mobile device and operation is
18 generated. The mobile device also generates event data defining events of the mobile device
19 for the associated mobile user. Such events are referred to as "Trigger points."

20 41. HTC IQAgent is programmed to obtain qualifying characteristics which may
21 include device type, such as manufacturer and model, available memory and battery life, the
22 type of applications resident on the device, the geographical location of the device, usage
23 statistics, including a "profile" that characterizes a user's interaction with a device, and the
24 profile. Such mobile device characteristics are referred to as "metrics."

25 42. Carrier IQ's patent for "data collection associated with components and services
26 of a wireless communication network" explains the breadth of this data collection,
27

28 Carrier IQ is able to query any metric from a device. A metric can be a
dropped call because of lack of service. The scope of the word metric is

1 very broad though, including device type, such as manufacturer and
2 model, available memory and battery life, the type of applications
3 resident on the device, the geographical location of the device, the end
4 user's pressing of keys on the device, usage history of the device,
5 including those that characterize a user's interaction with a device.

6 <http://www.fags.org/patents/app/20110106942> (last accessed December 2, 2011).

7 43. Carrier IQ provides a platform for data collection and management system to
8 dynamically generate and download to a population of wireless devices rule-based data
9 collection by coding its software to function when interfaced with "trigger points" and to
10 obtain "metrics." Data collection profiles may be generated manually by a network
11 administrator, a software developer or other personnel involved in the operation of the network
12 or "network administrators," created offline as a portion of a data analysis solution, or
13 automatically generated based on network.

14 44. This parameter data and event data may be used to monitor a network or used
15 by an advertising system of the mobile communications network to select an advertisement and
16 the timing of the display of the advertisement; and is necessary due to the problems associated
17 with mobile advertising.

18 45. Mobile Internet advertising currently consists of streaming graphic files, in real
19 time, into content rendered by a user's mobile device browser. Mobile advertising systems
20 though lack reliable browser tracking while traditional online advertising relies on the use of
21 browser cookies. Implementations inherent in conventional mobile ad serving have effectively
22 prevented mobile advertising from being effective because of its inability to obtain mobile
23 device "uniqueness." In order to obtain such uniqueness, the mobile advertising industry
24 sought a means to obtain unique device identifiers which provide a unique reference to
25 individual mobile devices. Unlike traditional cookies, such identifiers are hard coded into a
26 user's phones software, and thus a user has no ability to disable mobile device identifiers.

27 46. Mobile Device "tracking" by use of mobile device identifiers is not exactly
28 comparable to any other type of tracking by advertising networks. This is not anonymous data

1 – but an exact ID that's unique to each physical device, and if merged, with mobile device
2 activities, including but not limited to, identifying phone accessed user's physical locations,
3 time of transmission, applications downloaded, social network IDs, providing unlimited
4 advertising opportunities (i.e., commercial value). Recording of a user's GPS, without their
5 knowledge or consent also provides a security harm to the mobile device user. When tracking a
6 user's location data on the mobile device, it is calculated to eight decimal points that can be far
7 more exact and accurate than any sort of geographically-based IP address look-up on the web.
8 Instead of getting a general location, location data on a GPS-enabled mobile can identify user's
9 precise latitude and longitude.
10

11
12 47. The mobile device industry thus sought the technical means of synchronizing
13 tracking code so that information about individual consumer behavior on mobile devices could
14 be shared between companies and the unique device identifiers used in the majority of mobile
15 devices would be put to this purpose. Carrier IQ initial patent was able to extract unique

16 Identifiers from mobile devices:

17
18 Patent Title: COLLECTION OF DATA AT TARGET WIRELESS DEVICES USING DATA
19 COLLECTION PROFILES SYSTEMS AND METHODS FOR USING DISTRIBUTED
20 NETWORK ELEMENTS TO IMPLEMENT MONITORING AND DATA COLLECTION
21 CONCERNING SELECTED NETWORK PARAMETERS.

22 Patent No.: US 7,609,650 B2

23 Assignee: Carrier IQ, Inc., Mountain View, CA (US)

24 Filed: July 5, 2005

25 Inventor: Konstantin Othmer

26
27 48. The dilemma facing the mobile advertising industry is that once the mobile
28 device data was extracted a system and method was needed to for wireless devices to use data

1 for mobile advertising. Provided such a mechanism. While Carrier IQ may have concentrated
2 on extraction of mobile device metrics, other companies were interested in assisting the mobile
3 advertising networks to use mobile device data.

4
5 **C. HTC IQAgent Technology**

6 i. *HTC IQAgent Collection of Unencrypted User Data Via Device "Log File"*

7 49. Plaintiffs' independent investigation of the HTC IQAgent software revealed a
8 number of interesting factors not found in any study or account by HTC or Carrier IQ:

9 50. To monitor use of a mobile device, HTC IQAgent collects user data by utilizing
10 the mobile device's "log file"—a storage file that records certain actions or events that occur
11 on the device in real time, such as when the device is turned on or disconnected from a power
12 source. The log file can be examined by any software or application with Android operating
13 system permission to view it. Data is populated on the log file when software such as HTC IQ
14 Agent prompts the operating system to append an entry into the log file.

15 51. HTC IQAgent specifically prompts mobile operating systems to populate log
16 file data for a number of confidential events, including the following:

- 17
18 (a) the contents of all incoming text messages;
19 (b) the URLs of all websites visited; and
20 (c) a user's GPS coordinates.
21

22 HTC IQAgent records this data on the log file in an unencrypted format, so the data is
23 available to *any* device software or applications with log file permission. In other words, *any*
24 software or application with Android operating system access can transmit and collect the
25 user's incoming text messages, visited URLs and/or GPS coordinates because of the log file
26 entries populated by HTC IQAgent. This log file access is typically granted to software and
27 applications that a user installs from the market and a user would have no reason to believe
28 that in granting "log file" access, he or she is also granting access to this unencrypted,
confidential data.

1 52. This puts users' confidential data at great risk. Even if the authors of the
2 software and applications running on the mobile device have the best intentions, if these
3 authors incorporate any third party code into their own software or applications (which is quite
4 common), the users' data is exposed to these other third parties and is jeopardized.

5
6 ii. *HTC IQAgent Transmission of User Data Via Periodic Scheduling and*
7 *Remote Triggering*

8 53. HTC IQAgent provides two mechanisms to transmit confidential data off the
9 device: periodic scheduling and remote triggering. The HTC IQAgent software provides
10 specific "collection points" where the confidential data will be sent. One of these "collection
11 points" encoded in the software is http://collector.sky.carrieriq.com:7001/collector/c?cm_sl=5.
12 Data transmitted to this Carrier IQ server will remain unencrypted and unprotected during data
13 transmission and receipt.

14
15 54. HTC IQAgent can prompt a user's mobile device to send confidential data to
16 Carrier IQ's server on a periodic schedule, e.g., once a week or once a month. It can also
17 prompt a user's device to send confidential data at any time via a "WAP push request" or a
18 "text request." A WAP push request is a specially-formatted message delivered to the device
19 over a mobile data or internet connection requesting transmission of data from the device. A
20 user would be unaware that a WAP push request had been made to their device. A text request
21 is a standard text message sent to the device with contents beginning with "//CM" or "//IQ."
22 The contents of that message direct the device to transmit data from the device. This text
23 message is "suppressed" or hidden to the operator, meaning that the user does not see the text
24 message and is unaware that Carrier IQ or some other party has requested transmission of
25 confidential data from the device.

26
27
28 iii. *HTC IQAgent Continuous Unauthorized Data Logging and Transmission*

55. HTC IQAgent begins logging confidential user data the moment the user first

1 purchases the mobile device and turns it on, without notice to or consent from the user. HTC
2 IQAgent logs this data silently so that users have no knowledge the data is being logged or is
3 available to any device software or applications with log file permission. The data is also
4 transmitted silently so users are unaware that confidential data is being broadcast from their
5 devices. Data is logged and transmitted even when the device is not in use.

7 56. An average user will have no knowledge that the HTC IQAgent software is
8 even running on his or her device, and the HTC IQAgent software does not appear on the
9 device's application launch menu.

10 57. A user is unable to stop the Carrier IQ software from running. When a user
11 manually turns off the HTC IQAgent software, it automatically restarts itself seconds later. A
12 user is unable to delete or remove the HTC IQAgent software from the device without voiding
13 HTC's manufacturer's warranty.

15 58. The moment a device is turned on, HTC/Google checkin runs. This is
16 completely unrelated to "tell HTC." It sends data out on what the users flashed in recovery
17 (every file installed on a user's phone) IMEI, location and more. "Tell HTC" sends
18 "bugreport" information. This means that if a user of an HTC product has an issue they can
19 send HTC a report on it. HTC gives users an on "off switch" that allegedly allows a user to
20 stop the data collection.

22 59. One of the first data experts to recognize this was Trevor Eckhart. He noted
23 that HTC does not stop the data collection, it just stops the way it collects the data. HTC
24 continues to monitor actions and record events through other mechanisms on the phone. Mr.
25 Eckhart explained that

27
28 Carrier IQ is bundled as part of the HTC phone and does not appear in
any application menu or other software folder. The application itself is
called HTC IQAgent.apk. It's signed (protected) with HTC's crypto keys,

1 meaning HTC is not responsible for writing the code; however it has
2 been reported the URL sent data to is a not an HTC-owned URL.
3 "Carrier IQ also subverts standard operating system functionality. For
4 any application, I believe standard operating functionality includes
5 having a descriptively named application; a launcher icon, settings
6 menu, widget, or other method to allow the end user to access the
7 application; and a privacy policy clearly available on the device the
8 application is installed on. Also, as seen in the video, only an application
9 named HTC IQAgent is displayed as a running application on my HTC
10 device. A second program called IQRD never makes itself known as a
11 running application.";

12 CarrierIQ runs the binaries as user root in our ramdisk. The Carrier IQ
13 code is in almost every application: browser, dialer, SMS, media player,
14 the kernel itself, who knows where else.

15 Trevor Eckhart, Android Security Test, "Carrier IQ Information - Part #2," Online:

16 <http://cryptome.org/isp-spy/carrier-iq-spy2.pdf> (last accessed December 1, 2011).

17 60. Because the software is preinstalled by HTC and runs as part of the device
18 operating system, data is continuously collected and can be transmitted via wireless internet or
19 other means, even if the device user has no carrier contract and the mobile device is not
20 connected to a mobile network.

21 iv. *HTC IQAgent Depletion of Resources*

22 61. Because HTC IQAgent runs continuously and silently, it depletes device
23 resources without notice to or authorization from the user. These depleted resources include:

24 (a) battery power (required to run the device while activity such as data
25 logging and transmission occurs);

26 (b) device memory (used to log confidential user data and receive and
27 respond to WAP push requests and/or text requests);

28 (c) CPU (also known as "central processing unit" used to process the
instructions and perform the functions required by the HTC IQAgent software);

(d) bandwidth (used to transmit and receive data according to HTC
IQAgent instructions); and

(e) text messages (HTC IQAgent's hidden text request function indicates

1 a text has been received by the user even when the user cannot see it, and may result in a
2 charges to users who pay for a finite number of texts per month).

3 **D. HTC's Warranty**

4 62. There is no choice to "opt in" to Carrier IQ's data collection and transmission
5 by downloading HTC IQAgent since in many cases it is preinstalled or installed via automatic
6 update on Plaintiffs' and Class Members' mobile devices. Users cannot uninstall it, block it, or
7 cease its actions. HTC and Carrier IQ provide Plaintiffs and Class Members no notice of this
8 software or the functions it performs.
9

10 63. HTC's Manufacturer's Warranty for the HTC EVO states that the device is
11 designed to provide users with "reliable, worry-free service." It does not mention or disclose
12 the existence of the HTC IQAgent software on the device or the functions that software
13 performs.
14

15 64. HTC's Manufacturer's Warranty states that the Warranty will be void if a user
16 alters the operating system or opens or tampers with the device's outer casing, which would
17 include deleting or attempting to delete the HTC IQAgent software from the device.
18

19 **E. Defendants' Harmful Business Practices**

20 65. Defendants' business practice unfairly wrests the user's control and consumes
21 the resources of the Plaintiffs' and Class Members' mobile devices by gathering information,
22 populating such information in an unencrypted format in their mobile log file, and transferring
23 such information to storage for subsequent use. Defendants caused harm and damages to
24 Plaintiffs' and Class Members' mobile devices finite resources, depleted and exhausted its
25 battery power, memory, CPU bandwidth and text, thus causing an actual inability to use it for
26 its intended purposes and resulting in instability issues.
27

28 66. Defendants' collection and disclosure of this personal information violates user
expectations, diminished user's privacy, and contradicted the HTC's own representations.

1 These business practices are unfair and deceptive trade practices as set forth further below.

2 67. Defendants harmed Plaintiffs and Class Members when they purchased the
3 HTC device HTC IQAgent. In selecting the HTC mobile device over the service and goods of
4 other competing mobile phone manufacturers, Plaintiffs and Class Members reasonably
5 expected that their confidential user data would not be accessed and transmitted to third parties
6 without their knowledge and consent.

8 68. Defendants harmed Plaintiff and Class Members by obtaining their confidential
9 user data and device resources.

10 69. Carrier IQ exercises substantial control over its development and functionality
11 on HTC's mobile devices. Carrier IQ and HTC must agree to the terms of Carrier IQ's License
12 Agreement in order to have Carrier IQ function on HTC mobile device. Carrier IQ will only
13 function on mobile devices by interacting with a mobile device's operating system and features
14 in the ways permitted by such an agreement.

16 70. Carrier IQ's control of the user experience includes restrictions, such as
17 blocking consumers from modifying its software. As a direct consequence of the control
18 exercised by Carrier IQ, Plaintiffs and the Class cannot reasonably review the privacy effects
19 of HTC IQAgent.

21 71. Defendants' activities, made the basis of this action include, but are not limited
22 to, economic harm due to the unauthorized use of Plaintiffs' and Class Members' bandwidth,
23 the amount of data that can be transmitted across a channel in a set amount of time. Any
24 transmission of information on the internet includes bandwidth. Similar to utility companies,
25 such as power or water, the "pipeline" is a substantial capital expenditure, and bandwidth
26 usage controls the pricing model. Hosting providers charge user's for bandwidth because their
27 upstream provider charges them and so forth until it reaches the "back bone providers". Retail
28

1 providers purchase it from wholesalers to sell its consumers.

2 72. Defendants' activities made the basis of this action consume vast amounts of
3 bandwidth, slowing a user's internet connection by using their bandwidth, in addition to
4 diminishing the mobile devices "battery life," CPU and device memory in order to send, store
5 and retrieve metric data.
6

7 73. Plaintiffs and Class Members were afforded only a millisecond of time after
8 activating their HTC mobile device before HTC IQAgent intentionally, and without users'
9 authorization and consent, accessed Plaintiffs' and Class Members' mobile device. While only
10 the most tech savvy mobile device users are familiar with HTC IQAgent's activity, even a
11 more finite amount of individuals know how to actually remove HTC IQAgent, let alone
12 recognize the risk of that software to their confidential user data.
13

14 **VII. CLASS ACTION ALLEGATIONS**

15 74. Plaintiffs bring this action pursuant to Rule 23(a) and 23(b)(1)-(3) of the Federal
16 Rules of Civil Procedure on behalf of themselves and all others similarly situated, as members
17 of the proposed nationwide Class ("Nationwide Class"), defined as follows:
18

19 All consumers in the United States who purchased and used an HTC
20 mobile device on which the HTC IQAgent software resides from
December 4, 2007 to December 4, 2011.

21 75. Plaintiffs also bring certain of the claims on behalf of itself and a portion of the
22 class described as the Texas subclass ("Texas Subclass"), defined as follows:
23

24 All consumers residing within the State of Texas who purchased and
25 used an HTC mobile device on which the HTC IQAgent software
resides from December 4, 2007 to December 4, 2011.

26 76. Excluded from the Nationwide Class and Texas Subclass are the officers,
27 directors, and employees of Carrier IQ and HTC, and their respective legal representatives,
28 heirs, successors and assigns.

77. This action is brought as a class action and may properly be so maintained

1 pursuant to the provisions of Federal Rule of Civil Procedure 23. Plaintiffs reserve the right to
2 modify the Nationwide Class and the Texas Subclass definitions and the class period pursuant
3 to discovery that is conducted hereafter.

4 78. The members of the Class are so numerous that joinder of all members would
5 be impracticable. Plaintiffs estimate that there are hundreds of thousands of consumers who
6 purchased HTC mobile devices installed with the HTC IQAgent software.

7 79. There are questions of law and fact common to the members of the Class that
8 predominate over any questions affecting only individual members, including:

9 (a) whether Defendants omitted, misrepresented or otherwise failed to
10 notify Class Members of the fact that HTC IQAgent was installed on Plaintiffs' and Class
11 Members' mobile devices;

12 (b) whether Defendants omitted, misrepresented or otherwise failed to
13 notify Class Members of the fact that HTC IQAgent logs unencrypted data in the device log
14 file that includes incoming text messages, visited URLs and GPS location coordinates;

15 (c) whether Defendants omitted, misrepresented or otherwise failed to
16 notify Class Members of the fact that HTC IQAgent utilizes finite device resources such as
17 battery power, device memory, CPU, bandwidth and text messages;

18 (d) whether Defendants' conduct violates the federal Electronic
19 Communications Privacy Act

20 (e) whether Defendants' conduct violates the federal Stored
21 Communications Act;

22 (f) whether Defendants' conduct violates California's Consumers Legal
23 Remedies Act;

24 (g) whether Defendants' conduct violates Texas's Deceptive Trade
25 Practices Act;

26 (h) whether Defendants were negligent in their failure to disclose the
27 presence of HTC IQAgent on Plaintiffs' and Class Members' mobile devices and/or their
28 failure to seek Plaintiffs' and Class Members' consent prior to logging, collecting and

1 transmitting confidential user data;

2 (a) whether Defendants' conduct constitutes trespass; and

3 (b) whether Defendants were unjustly enriched from their conduct, and
4 whether they must disgorge profits to Plaintiffs and Class Members.

5 80. Plaintiffs' claims are typical of the claims of the members of the Class.
6 Plaintiffs have no interests antagonistic to those of the Class and are subject to no unique
7 defenses.

8 81. Plaintiffs will fairly and adequately protect the interests of the Class and have
9 retained attorneys experienced in class and complex litigation.

10 82. A class action is superior to other available methods for the fair and efficient
11 adjudication of this controversy for the following reasons:

12 (a) It is economically impractical for each member of the Class to
13 prosecute individual actions;

14 (b) The Class is readily definable;

15 (c) Prosecution as a class action will eliminate the possibility of
16 repetitious litigation;

17 (d) A class action will enable claims to be handled in an orderly and
18 expeditious manner;

19 (e) A class action will save time and expense and will ensure uniformity
20 of decisions; and

21 (f) Plaintiffs do not anticipate any difficulty in the management of this
22 litigation as a class action.

23 83. Defendants have acted and refused to act on grounds that apply generally to the
24 Class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting
25 the Class as a whole.

26
27 **VIII. CAUSES OF ACTION**

28 **FIRST CAUSE OF ACTION**

Violation of the Electronic Communications Privacy Act 18 U.S.C. § 2510

CLASS ACTION COMPLAINT

Against All Defendants

84. Plaintiffs incorporate by reference all paragraphs previously alleged herein.

85. Plaintiffs assert this claim against each and every Defendant named herein in this complaint on behalf of themselves and the Class.

86. The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510, referred to as "ECPA," regulates wire and electronic communications interception and interception of oral communications, and makes it unlawful for a person to "willfully intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication," within the meaning of 18 U.S.C. § 2511(1).

87. Defendants violated 18 U.S.C. § 2511 by intentionally acquiring and/or intercepting, by device or otherwise, Plaintiffs' and Class Members' electronic communications, without knowledge, consent, or authorization.

88. At all relevant times, Defendants engaged in business practices of intercepting and collecting the Plaintiffs' and Class Members' confidential electronic communications which included incoming text messages, URLs of websites viewed and GPS coordinates from within their mobile devices. Once Defendants obtained this confidential personal information, Defendants used it to aggregate mobile device data regarding Plaintiffs' and Class Members' uses of their mobile devices. Defendants also made this confidential and unencrypted data available to any device software or application with log file access, further violating Plaintiffs' and Class Members' privacy.

89. The contents of data transmissions from and to Plaintiffs' and Class Members' personal computers constitute "electronic communications" within the meaning of 18 U.S.C. § 2510.

90. Plaintiffs and Class Members are "person[s] whose ... electronic communication is intercepted ... or intentionally used in violation of this chapter" within the meaning of 18 U.S.C. § 2520.

91. Defendants violated 18 U.S.C. § 2511(1)(a) by intentionally intercepting, endeavoring to intercept, or procuring any other person to intercept or endeavor to intercept

1 Plaintiffs' and Class Members' electronic communications.

2 92. Defendants violated 18 U.S.C. § 2511(1)(c) by intentionally disclosing, or
3 endeavoring to disclose, to any other person the contents of Plaintiffs' and Class Members'
4 electronic communications, knowing or having reason to know that the information was
5 obtained through the interception of Plaintiffs' and Class Member's electronic
6 communications.

7 93. Defendants violated 18 U.S.C. § 2511(1)(d) by intentionally using, or
8 endeavoring to use, the contents of Plaintiffs' and Class Members' electronic communications,
9 knowing or having reason to know that the information was obtained through the interception
10 of Plaintiffs' and Class Members' electronic communications.

11 94. Defendants' intentional interception of these electronic communications without
12 Plaintiffs' or Class Members' knowledge, consent, or authorization was undertaken without a
13 facially valid court order or certification.

14 95. Defendants intentionally used such electronic communications, with knowledge,
15 or having reason to know, that the electronic communications were obtained through
16 interception, for an unlawful purpose.

17 96. Defendants unlawfully accessed and used, and voluntarily disclosed, the
18 contents of the intercepted communications to enhance their profitability and revenue through
19 manufacturer contracts and advertising. This access and disclosure was not necessary for the
20 operation of Defendants' system or to protect Defendants' rights or property.

21 97. The Electronic Communications Privacy Act of 1986, 18 USC §2520(a)
22 provides a civil cause of action to "any person whose wire, oral, or electronic communication
23 is intercepted, disclosed, or intentionally used" in violation of the ECPA.

24 98. Defendants are liable directly and/or vicariously for this cause of action.
25 Plaintiffs therefore seek remedy as provided for by 18 U.S.C. §2520, including such
26 preliminary and other equitable or declaratory relief as may be appropriate, damages consistent
27 with subsection (c) of that section to be proven at trial, punitive damages to be proven at trial,
28 and a reasonable attorney's fee and other litigation costs reasonably incurred.

100. Plaintiffs and the Class, pursuant to 18 U.S.C. §2520, are entitled to preliminary, equitable, and declaratory relief, in addition to statutory damages of the greater of \$10,000 or \$100 a day for each day of violation, actual and punitive damages, reasonable attorneys' fees, and Defendants' profits obtained from the above-described violations. Unless restrained and enjoined, Defendants will continue to commit such acts. Plaintiffs' and Class Members' remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Plaintiffs and Class Members to remedies including injunctive relief as provided by 18 U.S.C. § 2510.

Against All Defendants

104. Defendants intentionally accessed and collected the personal data of Plaintiffs

1 and Class Members on their mobile devices without notice or authorization, including
2 incoming text messages, URLs of websites viewed and GPS coordinates.

3 105. As a result of Defendants' unlawful violation of this section, Plaintiffs and Class
4 Members have been damaged by among other things, failing to receive the benefits of a
5 product impliedly represented to them as secure as to their personal information. Plaintiffs and
6 Class Members have additionally suffered loss by reason of these violations, including
7 violation of their rights of privacy. Defendants exposed Plaintiffs' and Class Members'
8 personal information to any third party software or application with log file access residing on
9 their mobile devices without Plaintiffs' or Class Members' permission or knowledge, and in an
10 unencrypted form. Plaintiffs and Class Members were damaged by Defendants' unauthorized
11 use of the resources of Plaintiffs' and Class Members' mobile devices including battery power,
12 cell phone memory, CPUs, and bandwidth. Moreover, Plaintiffs and Class Members had
13 unauthorized charges to their mobile devices for every hidden text message that was sent by
14 Defendants.
15

16 106. ~~Plaintiffs and Class Members have been harmed by Defendants' unlawful~~
17 violations of this section and are therefore entitled to relief in the form of damages, costs and
18 disbursements, including costs of investigation and reasonable attorney's fees and are entitled
19 to equitable relief as determined by this Court.

20 **THIRD CAUSE OF ACTION**

21 **Violation of the Consumer Legal Remedies Act**

22 **("CLRA") California Civil Code § 1750, et seq.**

23 **Against All Defendants**

24 107. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

25 108. In violation of Civil Code §1750, et seq. (the "CLRA"), Defendants have
26 engaged and are engaging in unfair and deceptive acts and practices in the course of
27 transactions with Plaintiffs, and such transactions are intended to and have resulted in the sales
28 of services to consumers. Plaintiffs and the Class Members are "consumers" as that term is
used in the CLRA because they sought or acquired Defendants' goods or services for personal,

1 family, or household purposes.

2 109. At all relevant times, Defendants' business practices of selling HTC mobile
3 devices installed or updated with HTC IQAgent software, were goods Plaintiffs and Class
4 Members obtained for use. Defendants' scheme to offer such goods misled Plaintiffs and Class
5 Members about the nature and integrity of the HTC mobile devices since Defendants intended
6 to use such for mobile device tracking, collection of confidential, unencrypted user data, and
7 depletion of consumer resources, including battery power, device memory, CPUs, and
8 bandwidth. Defendants also charged consumers for every hidden text message that was sent by
9 Defendants.

10 110. Defendants represented that their services had characteristics, uses, and benefits
11 that they do not have, in violation of Civil Code § 1770(a)(5). Defendants represented privacy
12 and "reliable, worry-free service" as a characteristic of the mobile devices that they did not
13 have. Defendants intercepted and collected Plaintiffs' and Class Members' electronic
14 communications which included incoming text messages, URLs of websites viewed and GPS
15 coordinates from within their mobile devices. Once Defendants obtained this personal
16 information, Defendants used it to aggregate mobile device data of Plaintiffs and Class
17 Members as they used their mobile device. Defendants made this personal information
18 available, unencrypted, to any third party software or applications with log file access on the
19 device and further violated Plaintiffs' and Class Members' privacy.
20

21 111. In addition, Defendants' modus operandi constitutes an unfair practice in that
22 Defendants knew, or should have known, that consumers care about the status of personal
23 information regarding visited websites, GPS location and text privacy but were unlikely to be
24 aware of the manner in which Defendants failed to fulfill their commitments with respect to the
25 consumers' privacy.

26 112. Defendants' acts and practices were deceptive and unfair because they were
27 likely to mislead the members of the public to whom they were directed.

28 113. Plaintiffs and Class Members have suffered loss by reason of these violations,
including, without limitation, violation of the right of privacy. Defendants exposed Plaintiffs'

1 and Class Members' personal information to any third party software or application with log
2 file access residing on their mobile devices without Plaintiffs' or Class Members' permission
3 or knowledge, and in an unencrypted form. Plaintiffs and Class Members were damaged by
4 Defendants' unauthorized use of the resources of Plaintiffs' and Class Members' mobile
5 devices including battery power, cell phone memory, CPUs, and bandwidth. Moreover,
6 Plaintiffs and Class Members had unauthorized charges to their mobile devices for every
7 hidden text message that was sent by Defendants.

8 114. Plaintiffs, on behalf of themselves and on behalf of each member of the Class,
9 shall seek individual restitution, injunctive relief, and other relief as the Court deems just and
10 proper.

11 115. Pursuant to California Civil Code, Section 1782, Plaintiffs will notify
12 Defendants in writing of the particular violations of Civil Code, Section 1770 and demand that
13 Defendants rectify the problems associated with its behavior detailed above, which acts and
14 practices are in violation of Civil Code Section 1770.

15 **FOURTH CAUSE OF ACTION**

16 **Violation of Unfair Competition California Business and Professions Code § 17200**

17 **Against All Defendants**

18 116. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

19 117. In violation of California Business and Professions Code Section 17200 et seq.,
20 Defendants' conduct in this regard is ongoing and includes, but is not limited to, unfair,
21 unlawful and fraudulent conduct.

22 118. At all relevant times, Defendants' business practices as alleged above constitute
23 unlawful, unfair and fraudulent business acts and practices.

24 119. Defendants engaged in these unfair and fraudulent practices to increase their
25 profits. Plaintiffs were injured and damaged by being forced to relinquish—without consent or
26 knowledge—confidential and personal user data, device battery power, device memory, CPUs,
27 and bandwidth. Plaintiffs were also unfairly charged for every hidden text message that was
28 sent by Defendants.

120. By engaging in the above-described acts and practices, Defendants have committed one or more acts of unfair competition within the meaning of the UCL and, as a result, Plaintiffs and the Class have suffered injury-in-fact and have lost money and/or property.

A. Unlawful Business Act and Practices

121. Defendants' business acts and practices are unlawful, in part, because they violate the Electronic Communications Privacy Act, 18 U.S.C. Section 2510 which prohibits any person from willfully intercepting or endeavoring to intercept, or procuring any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication, including incoming text messages.

122. Defendants' business acts and practices are also unlawful in that they violate the Stored Communications Act, 18 U.S.C. Section 2701, California Consumer Legal Remedies Act, California Civil Code §1750, and California Penal Code, § 502 among other statutes.

B. Unfair Business Act and Practices

123. Defendants' business acts and practices are unfair because they cause harm and injury-in-fact to Plaintiffs and Class Members and for which Defendants have no justification other than to increase revenues from the unauthorized use of personal information

124. Defendants' conduct lacks reasonable and legitimate justification in that Defendants have benefited from such conduct and practices while Plaintiffs and the Class Members have been misled as to the nature and integrity of Defendants' services and have, in fact, suffered injury regarding the privacy and confidentiality of their personal information and the use of their device resources. Defendants' conduct offends public policy in California in connection with the Consumer Legal Remedies Act, the state constitutional right of privacy, and California statutes recognizing the need for consumers to safeguard their own privacy interests, including California Civil Code, Section 1798.80.

125. In addition, Defendants' actions constitute an unfair practice in that Defendants knew, or should have known, that consumers care about the status of personal information regarding visited websites, GPS location and text privacy but were unlikely to be aware of the

1 manner in which Defendants failed to fulfill their commitments with respect to the consumers'
2 privacy.

3 126. Defendants' acts and practices were fraudulent within the meaning of the Unfair
4 Competition Law because they were likely to mislead the consumers.

5 127. Defendants' practice of capturing, storing, and transferring highly detailed and
6 personal records of consumers' incoming text messages, URLs of websites visited and GPS
7 location histories, and storing such information in unencrypted form, is in violation of the
8 Unfair Competition Law. Plaintiffs and Class Members have suffered loss by reason of these
9 violations, including, violation to their right of privacy. Defendants exposed Plaintiffs' and
10 Class Members' personal information to any third party software or applications with log file
11 access residing on their mobile devices without Plaintiffs' or Class Members' consent or
12 knowledge, and in an unencrypted form. Plaintiffs and Class Members were damaged by
13 Defendants' unauthorized use of the resources of Plaintiff's and Class Members' mobile
14 devices including battery power, cell phone memory, CPUs, and bandwidth. Moreover,
15 Plaintiffs and Class Members had to pay unauthorized charges to their mobile devices for
16 every hidden text message that was sent by Defendants.

17
18 **FIFTH CAUSE OF ACTION**

19 **Violation of California's Computer Crime Law**

20 **Penal Code § 502 et seq.**

21 **Against All Defendants**

22 128. Plaintiffs incorporate the above allegations by reference as if set forth herein at
23 length.

24 129. The California Computer Crime Law, California Penal Code Section 502
25 regulates "tampering, interference, damage, and unauthorized access to lawfully created
26 computer data and computer systems." A mobile device is a "computer system" as defined in
27 Penal Code Section 502(b)(5) in that it contains electronic instructions, inputs and outputs data,
28 performs functions including communication and data storage and retrieval.

130. Defendants violated California Penal Code § 502 by knowingly accessing,

1 copying, using, making use of, interfering, and/or altering, data belonging to Plaintiffs and
2 Class Members: (1) in and from the State of California; (2) in the home states of the Plaintiffs
3 and Class Members; and (3) in the state in which the servers that provided the communication
4 link between Plaintiffs and the applications they interacted with were located.

5 131. At all relevant times, Defendants had a business practice of accessing Plaintiffs'
6 and Class Members' mobile devices on a systematic and continuous basis in order to obtain
7 mobile device data and to monitor and collect data related to their browsing habits, GPS
8 locations and incoming text messages. Defendants accessed such data without notice to or
9 authorization from Plaintiffs or Class Members.

10 132. Pursuant to California Penal Code § 502(b)(1), "Access means to gain entry to,
11 instruct, or communicate with the logical, arithmetical, or memory function resources of a
12 computer, computer system, or computer network."

13 133. Pursuant to California Penal Code § 502(b)(6), "Data means a representation of
14 information, knowledge, facts, concepts, computer software, computer programs or
15 instructions. Data may be in any form, in storage media, or as stored in the memory of the
16 computer or in transit or presented on a display device."

17 134. Defendants have violated California Penal Code § 502(c)(1) by knowingly
18 accessing and without permission, altering, and making use of data from Plaintiffs' and Class
19 Members' mobile devices in order to devise and execute business practices to deceive
20 Plaintiffs and Class Members into surrendering private electronic communications, and to
21 wrongfully obtain valuable private data and device resources from Plaintiffs and Class
22 Members.
23

24 135. Defendants have violated California Penal Code § 502(c)(2) by knowingly
25 accessing and without permission, taking, or making use of data from Plaintiffs' and Class
26 Members' mobile devices.

27 136. Defendants have violated California Penal Code § 502(c)(3) by knowingly and
28 without permission, using and causing to be used Plaintiffs' and Class Members' mobile
computing devices' services and resources.

1 137. Defendants have violated California Penal Code section 502(c)(4) by knowingly
2 accessing and, without permission, adding and/or altering the data from Plaintiffs' and Class
3 Members' computers, including application code installed on such computers.

4 138. Defendants have violated California Penal Code § 502(c)(6) by knowingly and
5 without permission providing, or assisting in providing, a means of accessing Plaintiffs' mobile
6 device and mobile device system.

7 139. Defendants has violated California Penal Code § 502(c)(7) by knowingly and
8 without permission accessing, or causing to be accessed, Plaintiffs' mobile device and mobile
9 device system.

10 140. California Penal Code § 502(j) states: "For purposes of bringing a civil or a
11 criminal action under this section, a person who causes, by any means, the access of a
12 computer, computer system, or computer network in one jurisdiction from another jurisdiction
13 is deemed to have personally accessed the computer, computer system, or computer network in
14 each jurisdiction."

15 141. Plaintiffs and Class Members have suffered loss by reason of these violations,
16 including, without limitation, violation of the right of privacy. Defendants exposed Plaintiffs'
17 and Class Members' personal information to any third party software or application with log
18 file access residing on their mobile devices without Plaintiffs' or Class Members' permission
19 or knowledge, and in an unencrypted form. Plaintiffs and Class Members were damaged by
20 Defendants' unauthorized use of the resources of Plaintiff's and Class Members' mobile
21 devices including battery power, cell phone memory, CPUs, and bandwidth. Plaintiffs and
22 Class Members had unauthorized charges to their mobile devices for every hidden text
23 message that was sent by Defendants.

24 142. Plaintiffs have also suffered irreparable injury from these unauthorized acts of
25 disclosure, to wit: their personal, private, and sensitive electronic data was obtained and used
26 by Defendant. Due to the continuing threat of such injury, Plaintiffs have no adequate remedy
27 at law, entitling Plaintiffs to injunctive relief.

28 143. Plaintiffs and Class Members have additionally suffered loss by reason of these

1 violations, including, without limitation, violation of the right of privacy and depletion of
2 valuable device resources.

3 144. As a direct and proximate result of Defendants' unlawful conduct within the
4 meaning of California Penal Code § 502, Defendants have caused loss to Plaintiffs in an
5 amount to be proven at trial. Plaintiffs are also entitled to recover their reasonable attorneys'
6 fees pursuant to California Penal Code § 502(e).

7 145. Plaintiffs and the Class Members seek compensatory damages, in an amount to
8 be proven at trial, and injunctive or other equitable relief.

9 **SIXTH CAUSE OF ACTION**

10 **Violation of the California Invasion of Privacy Act**

11 **Penal Code § 630 et seq.**

12 **Against All Defendants**

13 146. Plaintiffs incorporate the above allegations by reference as if set forth herein at
14 length.

15 147. California Penal Code Section 630 provides, in part:

16 Any person who, . . . or who willfully and without the consent of
17 all parties to the communication, or in any unauthorized manner,
18 reads, or attempts to read, or to learn the contents or meaning of
19 any message, report, or communication while the same is in
20 transit or passing over any wire, line, or cable, or is being sent
21 from, or received at any place within this state; or who uses, or
22 attempts to use, in any manner, or for any purpose, or to
23 communicate in any way, any information so obtained, or who
24 aids, agrees with, employs, or conspires with any person or
25 persons to unlawfully do, or permit, or cause to be done any of
26 the acts or things mentioned above in this section, is punishable. .

27 148. At all relevant times, Defendants engaged in a business practice of accessing the
28 mobile device data of the Plaintiffs and Class Members without their authorization and consent
and systematically logging and collecting their incoming text messages, URLs of websites
viewed and GPS coordinates. Defendants made this personal data available to all third party
software or applications with log file access on the mobile devices of Plaintiffs and Class
Members in an unencrypted form, without the consent or authorization of Plaintiff or Class

1 Members.

2 149. On information and belief, each Plaintiff and each Class Member, during one or
3 more of their interactions on their mobile device, including receipt of text messages and URL
4 browsing, communicated with one or more web entities based in California, or with one or
5 more entities whose servers were located in California.

6 150. Communications from the California web-based entities to Plaintiffs and Class
7 Members were sent from California. Communications to the California web-based entities
8 from Plaintiffs and Class Members were sent to California.

9 151. Plaintiffs and Class Members did not consent to any of the Defendants' actions
10 in intercepting, reading, and/or learning the contents of their communications with such
11 California-based entities.

12 152. Plaintiffs and Class Members did not consent to any of the Defendants' actions
13 in using the contents of their communications with such California-based entities.

14 153. Neither Defendant is a "public utility engaged in the business of providing
15 communications services and facilities . . ."

16 154. The actions alleged herein by the Defendants were not undertaken "for the
17 purpose of construction, maintenance, conduct or operation of the services and facilities of the
18 public utility."

19 155. The actions alleged herein by the Defendants were not undertaken in connection
20 with "the use of any instrument, equipment, facility, or service furnished and used pursuant to
21 the tariffs of a public utility."

22 156. The actions alleged herein by Defendants were not undertaken with respect to
23 any telephonic communication system used for communication exclusively within a state,
24 county, city and county, or city correctional facility.

25 157. Defendants directly participated in intercepting, reading, and/or learning the
26 contents of the communications between Plaintiffs, Class Members and California-based web
27 entities.
28

158. Alternatively, and of equal violation of the California Invasion of Privacy Act,

1 HTC aided, agreed with, and/or conspired with Carrier IQ to unlawfully do, or permit, or cause
2 to be done all of the acts complained of herein.

3 159. Plaintiffs and Class Members have additionally suffered loss by reason of these
4 violations, including, without limitation, violation of the right of privacy. Defendants exposed
5 Plaintiffs' and Class Members' personal information to any third party software or application
6 with log file access residing on their mobile devices without Plaintiffs' or Class Members'
7 permission or knowledge, and in an unencrypted form. Plaintiffs and Class Members were
8 damaged by Defendants' unauthorized use of the resources of Plaintiff's and Class Members'
9 mobile devices including battery power, cell phone memory, CPUs, and bandwidth. Moreover,
10 Plaintiffs and Class Members had unauthorized charges to their mobile devices for every
11 hidden text message that was sent by Defendants.

12 160. Unless restrained and enjoined, Defendants will continue to commit such acts.
13 Pursuant to § 637.2 of the California Penal Code, Plaintiffs and the Class have been injured by
14 the violations of California Penal Code Section 631. Wherefore, Plaintiffs, on behalf of
15 themselves and on behalf of a similarly situated Class of consumers, seek damages and
16 injunctive relief.

17 **SEVENTH CAUSE OF ACTION**

18 **Violation of the Song-Beverly Warranty Act, California Civil Code §1792**

19 **Against All Defendants**

20
21 161. Plaintiffs hereby incorporate by reference the allegations contained in all the
22 paragraphs of this Complaint.

23 162. HTC warranted to Plaintiffs and Class Members in its "Manufacturer's
24 Warranty" that the mobile devices would be free from defects for normal consumer usage for
25 twelve months from the date of purchase.

26 163. HTC by offering mobile devices in the marketplace represented and warranted
27 to Plaintiffs and Class Members that these devices did not cause personal information to be
28 unreasonably and unexpectedly transferred to third parties.

164. Plaintiffs and Class Members paid more for their mobile devices than they

1 would have paid if HTC disclosed the fact that the mobile devices were designed with defects,
2 namely the privacy breach to Carrier IQ and any other third party software on the mobile
3 device.

4 165. A reasonable consumer would, and Plaintiffs and Class Members did expect
5 that, if HTC mobile devices were subject to defects such as those identified above, HTC would
6 disclose these material facts and Plaintiffs and Class Members would not have purchased these
7 devices.

8 166. Plaintiffs and Class Members paid premiums for HTC mobile devices because
9 they reasonably believed the devices were designed to employ reasonable security in their
10 operation.

11 167. HTC's failure to meet the specifications of the mobile devices violates the
12 express and implied warranties under the Song-Beverly Warranty Act, California Civil Code
13 §1792 et seq.

14 168. Moreover, HTC asserts that disabling the Carrier IQ software on a mobile
15 device voids the HTC Warranty. Plaintiffs and Class Members are therefore forced to induce
16 breach of the HTC Warranty by disabling the Carrier IQ software to protect their personal
17 information.

18 169. Plaintiffs and Class Members who purchased the mobile devices are entitled to
19 a refund of the purchase price.
20

21 **EIGHTH CAUSE OF ACTION**

22 **Texas Deceptive Trade Practices Act, Business and Commerce**

23 **Code § 17.41 et seq.**

24 **Against All Defendants**

25 170. Plaintiffs hereby incorporate by reference the allegations contained in all of the
26 preceding paragraphs of this complaint.

27 171. Plaintiffs are "consumers" under the Texas Deceptive Trade Practices Act as
28 they purchased and used HTC mobile devices that had been preinstalled with the Carrier IQ
tracking program.

CLASS ACTION COMPLAINT

1 172. Defendants are proper "persons" or defendants under the Texas Deceptive
2 Trade Practices Act, who either used or employed false, misleading, deceptive or
3 unconscionable acts or practices, or were directly connected with the transaction with
4 Plaintiffs.

5 173. Defendants committed multiple violations and wrongful acts under the Texas
6 Deceptive Trade Practices Act, including the following: making or committing, false,
7 misleading or deceptive acts and/or practices, including but not limited to violations of Tex.
8 Business & Commerce Code § 17.46(b) (3), (5), (7), (9), (20), and (24). Defendants committed
9 misleading and unconscionable acts in connection with the sale of mobile devices installed or
10 updated with HTC IQAgent to Plaintiffs and Class Members, and the subsequent tracking and
11 logging of Plaintiffs' and Class Members' confidential, unencrypted through HTC IQAgent
12 without notice or consent. In carrying out these acts, Defendants depleted Plaintiffs' and Class
13 Members' mobile device resources without notice to or consent from Plaintiffs or Class
14 Members. Plaintiffs and Class Members relied on Defendants' acts and/or practices to their
15 detriment.

16 174. Plaintiffs will show that the violation and actions of Defendants were a
17 producing cause of their damages. Defendants exposed Plaintiffs' and Class Members'
18 personal information to any third party software or applications with log file access residing on
19 their mobile devices without Plaintiffs' or Class Members' permission or knowledge, and in an
20 unencrypted form. Plaintiffs and Class Members were damaged by Defendants' unauthorized
21 use of Plaintiffs' and Class Members' mobile device resources including battery power, cell
22 phone memory, CPUs, and bandwidth. Moreover, Plaintiffs and Class Members had
23 unauthorized charges to their mobile devices for every hidden text message that was sent by
24 Defendants.

25 175. Plaintiffs will show that the violations and actions of Defendants were done
26 intentionally or knowingly, entitling Plaintiffs to treble damages.

27 176. Plaintiffs will show that the violations and actions of Defendants entitle them to
28 reasonable and necessary attorney's fees under the Texas Deceptive Trade Practices Act,

specifically Tex. Business & Commerce Code § 17.50(d).

NINTH CAUSE OF ACTION

Breach of Express Warranty

Against Defendant HTC

177. Plaintiffs hereby incorporate by reference the allegations contained in all the paragraphs of this Complaint.

178. HTC warranted to Plaintiffs and Class Members in its "Manufacturer's Warranty" that the mobile devices would be free from defects for normal consumer usage for twelve months from the date of purchase and that the device was designed to provide "reliable, worry-free service."

179. HTC by sold mobile devices to Plaintiffs and Class Members that were defective because they caused personal information to be unreasonably and unexpectedly viewed and collected by Carrier IQ and other third party software and applications. The devices also were subject to depletion of resources through the HTC IQAgent software which depleted those resources without notice to or authorization from Plaintiffs or Class Members.

180. Plaintiffs and Class Members paid more for their mobile devices than they would have paid if HTC disclosed the fact that the mobile devices were designed with defects, namely the privacy breach and depletion of mobile device resources.

181. A reasonable consumer would, and Plaintiffs and Class Members did expect that, if HTC mobile devices were subject to defects such as those identified above, HTC would disclose these material facts and Plaintiffs and Class Members would not have purchased these devices.

182. Plaintiffs and Class Members paid premiums for HTC mobile devices because they reasonably believed the devices were designed to employ reasonable security in their operation.

183. HTC's failure to provide to Plaintiffs and Class Members a mobile device that is not defective is a violation of HTC's express warranty.

184. Moreover, HTC asserts that disabling the Carrier IQ software on a mobile

1 device voids the HTC warranty. Plaintiffs and Class Members are therefore forced by HTC to
2 induce breach of the HTC Warranty by disabling the Carrier IQ software to protect their
3 personal information.

4 185. Plaintiffs and Class Members who purchased the mobile devices are entitled to
5 a refund of the purchase price.

6 **TENTH CAUSE OF ACTION**

7 **Breach of Implied Warranty**

8 **Against Defendant HTC**

9 186. Plaintiffs hereby incorporate by reference the allegations contained in all the
10 paragraphs of this Complaint.

11 187. HTC by offering mobile devices in the marketplace represented and warranted
12 to Plaintiffs and Class Members that these devices would be free from defects for normal
13 consumer usage and would not cause personal information to be unreasonably and
14 unexpectedly transferred to third parties.

15 188. HTC by sold mobile devices to Plaintiffs and Class Members that were
16 defective because they caused personal information to be unreasonably and unexpectedly
17 viewed and collected by Carrier IQ and other third party software and applications. The
18 devices also were subject to depletion of resources through the HTC IQAgent software which
19 depleted those resources without notice to or authorization from Plaintiffs or Class Members.
20

21 189. Plaintiffs and Class Members paid more for their mobile devices than they
22 would have paid if HTC disclosed the fact that the mobile devices were designed with defects,
23 namely the privacy breach and depletion of mobile device resources..

24 190. A reasonable consumer would, and Plaintiffs and Class Members did expect
25 that, if HTC mobile devices were subject to defects such as those identified above, HTC would
26 disclose these material facts and Plaintiffs and Class Members would not have purchased these
27 devices.

28 191. Plaintiffs and Class Members paid premiums for HTC mobile devices because
they reasonably believed the devices were designed to employ reasonable security in their

1 operation.

2 192. HTC's failure to provide to Plaintiffs and Class Members a mobile device that is
3 not defective is a violation of HTC's implied warranty.

4 193. Plaintiffs and Class Members who purchased the mobile devices are entitled to
5 a refund of the purchase price.

6 **ELEVENTH CAUSE OF ACTION**

7 **Negligence**

8 **Against All Defendants**

9 194. Plaintiffs incorporate the above allegations by reference as if fully set forth
10 herein.

11 195. Carrier IQ and HTC owed a duty of care to Plaintiffs and Class Members.

12 196. Carrier IQ and HTC breached their duty by negligently designing HTC IQAgent
13 and preinstalling or uploading it to Plaintiffs' and Class Members' mobile devices without any
14 notice or authorization so that Defendants could acquire personal information without
15 Plaintiffs' and Class Members' knowledge or permission. Defendants also negligently made
16 this confidential data available to any software or application with log file access on the mobile
17 device, in an unencrypted format. Defendants also negligently depleted Plaintiffs' and Class
18 Members' mobile device resources.

19 197. Carrier IQ and HTC failed to fulfill their own commitments to Plaintiffs and
20 Class Members, and further failed to fulfill even the minimum duty of care to protect
21 Plaintiffs' and Class Members' personal information, privacy rights, security, and device
22 resources.

23 198. HTC's unencrypted storage of Plaintiffs' and Class Members' on the mobile
24 device log file and Carrier IQ servers was negligent.

25 199. Plaintiffs and Class Members were harmed as a result of Carrier IQ's breaches
26 of its duty, and Carrier IQ proximately caused such harms.

27 200. HTC's failure to fulfill its commitments included allowing Carrier IQ's practice
28 of preinstalling HTC IQAgent on HTC mobile device users' devices without notice or

1 authorization and then permitting Carrier IQ to collect unencrypted data in the log file and
2 make it available, unencrypted, to third party software and applications with log file access on
3 the devices. HTC engaged in these activities without notice to or consent from Plaintiffs and
4 Class Members.

5 201. HTC's preinstallation or upload of HTC IQAgent and unauthorized use of
6 Plaintiffs' and Class Members' confidential information without notice to or consent from
7 Plaintiffs or Class Members was negligent.

8 202. Defendants exposed Plaintiffs' and Class Members' personal information to any
9 third party software with log file access residing on their mobile devices without Plaintiffs' or
10 Class Members' permission or knowledge, and in an unencrypted form. Plaintiffs and Class
11 Members were damaged by Defendants' unauthorized use of the resources of their mobile
12 devices including battery power, cell phone memory, CPUs, and bandwidth. Moreover,
13 Plaintiffs and Class Members had unauthorized charges to their mobile devices for every
14 hidden text message that was sent by Carrier IQ.

15 203. Plaintiffs and Class Members were harmed as a result of Defendants' breaches
16 of their duty, and Defendants proximately caused such harms.

17 **TWELFTH CAUSE OF ACTION**

18 **Trespass to Personal Property/Chattels**

19 **Against All Defendants**

20 204. Plaintiffs incorporate by reference all paragraphs previously alleged herein.

21 205. The common law prohibits the intentional intermeddling with personal property,
22 including a mobile device, in possession of another which results in the deprivation of the use
23 of the personal property or impairment of the condition, quality, or usefulness of the personal
24 property.

25 206. By engaging in the acts alleged in this complaint without the authorization or
26 consent of Plaintiffs and Class Members, Defendants dispossessed Plaintiffs and Class
27 Members from use and/or access to their mobile devices, or parts of them. Further, these acts
28 impaired the use, value, and quality of Plaintiffs' and Class Members' mobile devices.

1 Defendants' acts constituted an intentional interference with the use and enjoyment of their
2 mobile devices. By the acts described above, Defendants have repeatedly and persistently
3 engaged in trespass to personal property in violation of the common law.

4 207. Without Plaintiffs' and Class Members' consent, or in excess of any consent
5 given, Defendants knowingly and intentionally accessed Plaintiffs' and Class Members'
6 property, thereby intermeddling with Plaintiffs' and Class Members' right to possession of the
7 property and causing injury to Plaintiffs and the members of the Class.

8 208. Defendants engaged in deception and concealment in order to gain access to
9 Plaintiffs' and Class Members' mobile devices.

10 209. Defendants undertook the following actions with respect to Plaintiffs' and Class
11 Members' mobile devices:

12 210. Defendants accessed and obtained control over the users' mobile device;

13 211. Defendants caused the installation of code on the hard drives of the mobile
14 devices;

15 212. Defendants programmed the operation of its code to circumvent the mobile
16 device owners' privacy and security controls, to remain beyond their control, and to continue
17 to function and operate without notice to them, or consent from Plaintiffs and Class Members;

18 213. Defendants obtained users' personal information by logging confidential data in
19 the log file;

20 214. Defendants utilized users' mobile device resources as part of logging
21 confidential data; and

22 215. Defendants used the log file data to obtain information about the mobile
23 browsing activities of the mobile device without the user's consent, and outside of the control
24 of the owner of the mobile device.

25 216. All these acts described above were acts in excess of any authority any user
26 granted Defendants when the user purchased the HTC mobile device that had HTC IQAgent
27 preinstalled or updated on the device without the user's consent or knowledge. By engaging in
28 deception and misrepresentation, whatever authority or permission Plaintiffs and Class

1 Members may have granted to Defendants was exceeded.

2 217. Defendants' installation and operation of its program used, interfered, and/or
3 intermeddled with Plaintiffs' and Class Members' mobile devices. Such use, interference
4 and/or intermeddling was without Plaintiffs' and Class Members' consent or, in the alternative,
5 in excess of Plaintiffs' and Class Members' consent.

6 218. Defendants' installation and operation of its program constitutes trespass,
7 nuisance, and an interference with Plaintiffs' and Class Members' chattels, to wit, their mobile
8 devices.

9 219. Defendants' installation and operation of the Carrier IQ program impaired the
10 condition and value of Plaintiffs' and Class Members' mobile devices.

11 220. Defendants' trespass to chattels, nuisance, and interference caused real and
12 substantial damage to Plaintiffs and Class Members. Defendants exposed Plaintiffs' and Class
13 Members' personal information to any third party software with log file access residing on
14 their mobile devices without Plaintiffs' or Class Members' permission or knowledge, and in an
15 unencrypted form. Plaintiffs and Class Members were damaged by Defendants' unauthorized
16 use of the resources of Plaintiffs' and Class Members' mobile devices including battery power,
17 cell phone memory, CPUs, and bandwidth. Plaintiffs and Class Members had unauthorized
18 charges to their mobile devices for every hidden text message that was sent by Carrier IQ.

19 221. As a direct and proximate result of Defendants' trespass to chattels, nuisance,
20 interference, unauthorized access of and intermeddling with Plaintiffs' and Class Members'
21 property, Defendants have injured and impaired Plaintiffs and Class Members in the condition
22 and value of Plaintiffs' Class Members' mobile devices, as follows:

23 (a) By consuming the resources of and/or degrading the performance of
24 Plaintiffs' and Class Members' mobile devices (including space, memory, processing cycles,
25 Internet connectivity, and unauthorized use of their bandwidth);

26 (b) By diminishing the use of, value, speed, capacity, and/or capabilities
27 of Plaintiffs' and Class Members' mobile devices;

28 (c) By devaluing, interfering with, and/or diminishing Plaintiffs' and

1 Class Members' possessory interest in their mobile devices;

2 (d) By altering and/or controlling the functioning of Plaintiffs' and Class
3 Members' mobile devices;

4 (e) By infringing on Plaintiffs' and Class Members' right to exclude
5 others from their mobile devices;

6 (f) By infringing on Plaintiffs' and Class Members' right to determine, as
7 owners of/or their mobile devices, which programs should be installed and operating on their
8 mobile devices;

9 (g) By compromising the integrity, security, and ownership of Class
10 Members' mobile devices; and

11 (h) By utilizing Plaintiffs' and Class Members' mobile device resources
12 without notice or consent.

13 **THIRTEENTH CAUSE OF ACTION**

14 **Unjust Enrichment**

15 **Against All Defendants**

16 222. Plaintiffs hereby incorporate by reference the allegations contained in all of the
17 paragraphs of this complaint.

18 223. By engaging in the conduct described in this Complaint, Defendants have
19 knowingly obtained benefits from the Plaintiffs and Class Members under circumstances that
20 make it inequitable and unjust for Defendants to retain them.

21 224. Plaintiffs and the Class have conferred a benefit upon the Defendants who have,
22 directly or indirectly, received and retained the confidential information of Plaintiffs and Class
23 Members as set forth herein. Defendants have received and retained information that is
24 otherwise private, confidential, and not of public record, and/or have received revenue from the
25 provision, use, and or trafficking in the sale of such information.

26 225. Defendants appreciate and/or have knowledge of said benefit.

27 226. Under principles of equity and good conscience, Defendants should not be
28 permitted to retain the information and/or revenue that they acquired by virtue of their

1 unlawful conduct. All funds, revenue, and benefits received by them rightfully belong to
2 Plaintiffs and the Class, which the Defendants have unjustly received as a result of their
3 actions.

4 227. Plaintiffs and Class Members have no adequate remedy at law.

5 228. Defendants have received a benefit from Plaintiffs and Class Members and
6 Defendants have received and retained money or other benefits from third parties as a result of
7 sharing Plaintiffs' and Class Members' confidential information of Plaintiffs and Class
8 Members without Plaintiffs' or Class Members' knowledge or consent as alleged in this
9 Complaint.

10 229. Plaintiffs and Class Members did not expect that Defendants would seek to gain
11 commercial or business advantage from third parties by using their personal information
12 without their knowledge or consent.

13 230. Defendants knowingly used Plaintiffs' and Class Members' confidential
14 information without their knowledge or consent to gain commercial advantage from third
15 parties and had full knowledge of the benefits they have received from Plaintiffs and Class

16 Members. If Plaintiffs and Class Members had known Defendants were not keeping their
17 confidential information from third-parties, they would not have consented and Defendants
18 would not have gained commercial or business advantage from third parties.

19 231. Defendants will be unjustly enriched if Defendants are permitted to retain the
20 money or other benefits paid to them by third parties, or resulting from the commercial or
21 business advantage they gained, in exchange for Plaintiffs' and Class Members' confidential
22 information.

23 232. Defendants should be required to provide restitution of all money obtained from
24 their unlawful conduct.

25 233. Plaintiffs and the Members of the Class are entitled to an award of
26 compensatory and punitive damages in an amount to be determined at trial or to be imposition
27 of a constructive trust upon the wrongful revenues and/or profits obtained by and benefits
28 conferred upon Defendants as a result of the wrongful actions as alleged in this complaint.

1 234. Plaintiffs and the Class have no remedy at law to prevent Defendants from
2 continuing the inequitable conduct alleged in this complaint and the continued unjust retention
3 of the money and/or benefits Defendants received from third parties.

4 **FOURTEENTH CAUSE OF ACTION**

5 **Conversion**

6 **Against All Defendants**

7 235. Plaintiffs hereby incorporate by reference the allegations contained in all of the
8 preceding paragraphs of this complaint.

9 236. Plaintiffs' and Class Members' mobile device data, including but not limited to
10 their incoming text messages, URLs of websites viewed and GPS coordinates, was viewed by
11 Defendants and made available to third party software and applications with log file permission
12 to collect confidential, unencrypted data about Plaintiffs' and Class Members' mobile device
13 activities. Such property, owned by the Plaintiffs and Class Members, is valuable to the
14 Plaintiffs and Class Members.

15 237. Plaintiffs' and Class Members' mobile devices use battery power, cell phone
16 memory, CPUs, and bandwidth. Defendants' activities, made the basis of this action, used
17 without notice or authorization, such battery power, memory, CPU and bandwidth for purposes
18 not contemplated and not agreed to by Plaintiffs and Class Members when they purchased their
19 HTC mobile devices. Such property, owned by Plaintiffs and Class Members, is valuable to
20 Plaintiffs and Class Members. Plaintiffs and Class Members were damaged by Defendants'
21 unauthorized use of Plaintiff's and Class Members' battery power, cell phone memory and
22 CPUs, as well as bandwidth. Moreover, Defendants utilized Plaintiffs' and Class Members'
23 limited text messages in order to send secret and unauthorized instructions to their mobile
24 devices. Plaintiffs and Class Members paid unauthorized charges for every hidden text
25 message that was sent by Defendants.
26

27 238. Defendants unlawfully exercised dominion over said property and thereby
28 converted Plaintiffs' and Class Members' property.

 239. Plaintiffs and Class Members were damaged by Defendants' actions.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for judgment against Defendants as follows:

A. Certify this case as a Class action on behalf of the Classes defined above, appoint Plaintiffs as Class representatives, and appoint their counsel as Class counsel;

B. Declare that the actions of Defendants, as set out above, violate the claims alleged;

C. Award injunctive and equitable relief including, *inter alia*: (i) prohibiting Defendants from engaging in the acts alleged above; (ii) requiring Defendants to disgorge all of their ill-gotten gains to Plaintiffs and Class Members, or to whomever the Court deems appropriate; (iii) requiring Defendants to delete all data surreptitiously or otherwise collected data through the acts alleged above; (iv) requiring Defendants to provide Plaintiffs and Class Members a means to easily and permanently decline any participation in any data collection activities; (v) awarding Plaintiffs and Class Members full restitution of all benefits wrongfully acquired by Defendants by means of the wrongful conduct alleged herein; and (vi) ordering an accounting and constructive trust imposed on the data, funds, or other assets obtained by unlawful means as alleged above, to avoid dissipation, fraudulent transfers, and/or concealment of such assets by Defendants;

D. Award damages, including statutory damages where applicable, to Plaintiffs and Class Members in an amount to be determined at trial;

E. Award restitution against Defendants for all money to which Plaintiffs and the Classes are entitled in equity;

F. Restrain Defendants, their officers, agents, servants, employees, and attorneys, and those in active concert or participation with them from continued access, collection, and transmission of Plaintiffs' and Class Members' confidential user data via preliminary and permanent injunction;

G. Award Plaintiffs and the Classes:

(i) Compensatory damages sustained by Plaintiffs and all others

CLASS ACTION COMPLAINT

1 similarly situated as a result of Defendants' unlawful acts and conduct;

2 (j) Restitution, disgorgement and/or other equitable relief as the
3 Court deems proper;

4 (k) Plaintiffs' reasonable litigation expenses and attorneys' fees;

5 (l) Pre- and post-judgment interest, to the extent allowable;

6 (m) Statutory damages, including punitive damages; and

7 (n) Permanent injunction prohibiting Defendants from engaging
8 in the conduct and practices complained of herein.

9 For such other and further relief as this Court may deem just and proper.

10 Dated this 6th day of December, 2011.

11
12 
13 By: _____

14 STRANGE & CARPENTER

15 Brain R. Strange (Cal. Bar. No. 103252)
16 LACounsel@earthlink.net
17 12100 Wilshire Boulevard, Suite 1900
18 Los Angeles, CA 90025
19 Telephone: (310) 207-5055
20 Facsimile: (310) 826-3210

21 Law Office of Joseph H. Malley
22 Joseph H. Malley (not admitted)
23 malleylaw@gmail.com
24 1045 North Zang Blvd
25 Dallas, TX 75208
26 Telephone: (214) 943-6100

27 *Counsel for Plaintiffs and the Proposed Class*
28

JURY TRIAL DEMAND

The Plaintiffs hereby demand a trial by jury of all issues so triable.

Dated this 6th day of December, 2011.

By: 

STRANGE & CARPENTER

Brain R. Strange (Cal. Bar. No. 103252)
LACounsel@earthlink.net
12100 Wilshire Boulevard, Suite 1900
Los Angeles, CA 90025
Telephone: (310) 207-5055
Facsimile: (310) 826-3210

Law Office of Joseph H. Malley
Joseph H. Malley (not admitted)
malleylaw@gmail.com
1045 North Zang Blvd
Dallas, TX 75208
Telephone: (214) 943-6100

Counsel for Plaintiffs and the Proposed Class

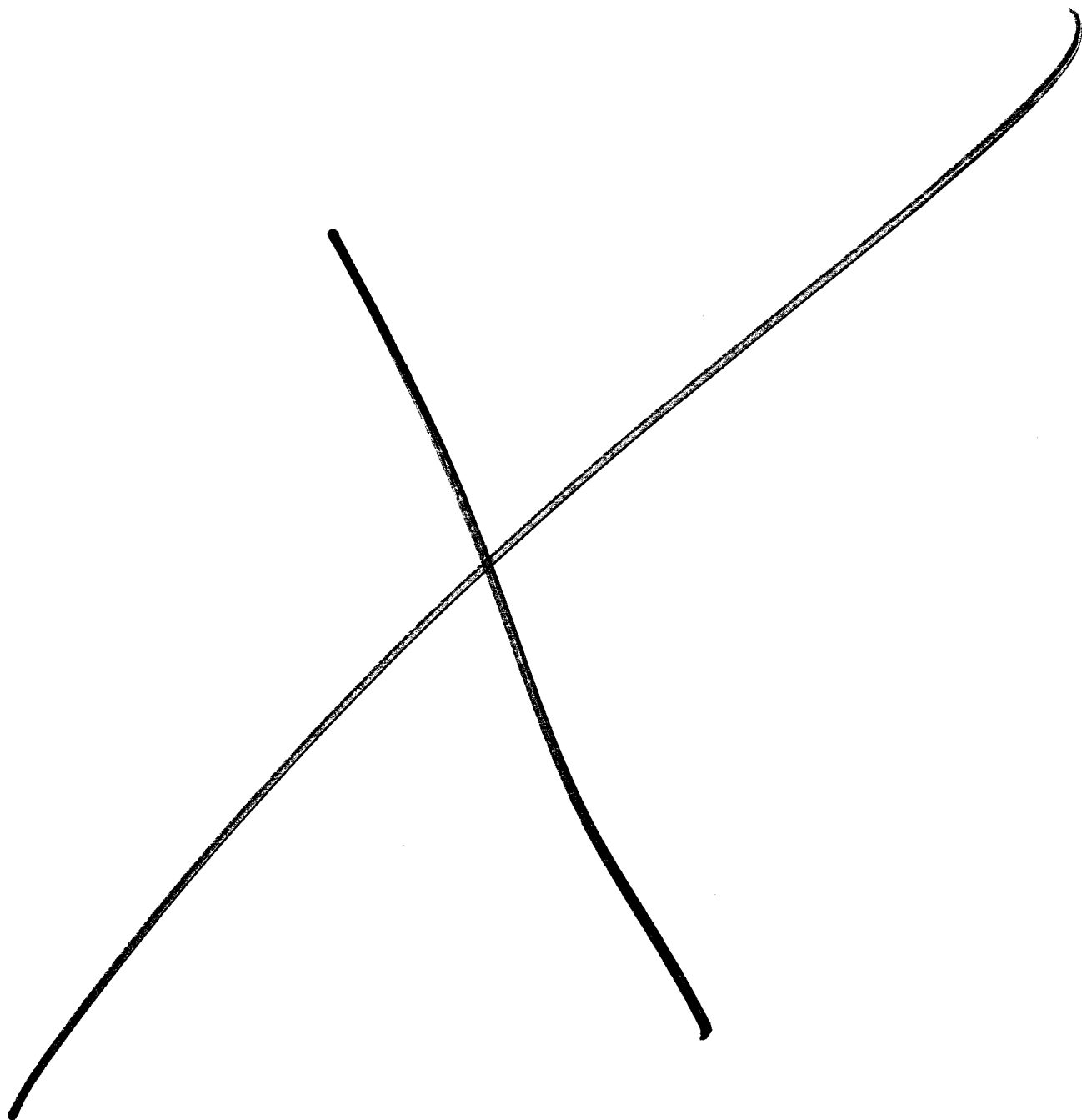


Exhibit 3:

Phong v. Carrier IQ, Inc., et al.

**U.S. District Court
California Northern District (San Jose)
CIVIL DOCKET FOR CASE #: 5:11-cv-06333-HRL**

Phong v. Carrier IQ, Inc et al
Assigned to: Magistrate Judge Howard R. Lloyd
Cause: 28:1331 Fed. Question

Date Filed: 12/14/2011
Jury Demand: Plaintiff
Nature of Suit: 890 Other Statutory
Actions
Jurisdiction: Federal Question

Plaintiff

Dao Phong
*an individual, on behalf of herself and
all others similarly situated*

represented by **Mark Punzalan**
Finkelstein, Thompson LLP
100 Bush Street
Suite 1450
San Francisco, CA 94104
415-398-8700
Fax: 415-398-8704
Email: mpunzalan@finkelsteinthompson.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Danielle A Stoumbos
Finkelstein Thompson, LLP
100 Bush Street
Suite 1450
San Francisco, CA 94104
415-398-8700
Fax: 415-398-8704
Email: dstoumbos@finkelsteinthompson.com
ATTORNEY TO BE NOTICED

Rosemary M. Rivas
Finkelstein Thompson LLP
100 Bush Street
Suite 1450
San Francisco, CA 94104
415-398-8700
Fax: 415-398-8704
Email: rrivas@finkelsteinthompson.com
ATTORNEY TO BE NOTICED

V.

Defendant

Carrier IQ, Inc

Defendant

HTC America, Inc.

Date Filed	#	Docket Text
12/14/2011	<u>1</u>	Alleged Class Action Complaint (Summons Issued; jury demand; against Carrier IQ, Inc, HTC America, Inc. (Filing fee \$ 350, receipt number 54611011012). Filed by Dao Phong. (Attachments: # <u>1</u> Civil Cover Sheet) (bw, COURT STAFF) (Filed on 12/14/2011) (Entered: 12/15/2011)
12/14/2011	<u>2</u>	Summons Issued as to Carrier IQ, Inc. (bw, COURT STAFF) (Filed on 12/14/2011) (Entered: 12/15/2011)

12/14/2011	<u>3</u>	Summons Issued as to HTC America, Inc.. (bw, COURT STAFF) (Filed on 12/14/2011) (Entered: 12/15/2011)
12/14/2011	<u>4</u>	ADR SCHEDULING ORDER: Case Management Statement due by 3/6/2012. Case Management Conference set for 3/13/2012 01:30 PM in Courtroom 2, 5th Floor, San Jose. (bw, COURT STAFF) (Filed on 12/14/2011) (Entered: 12/15/2011)
12/14/2011		CASE DESIGNATED for Electronic Filing. (bw, COURT STAFF) (Filed on 12/14/2011) (Entered: 12/15/2011)
12/19/2011	<u>5</u>	Administrative Motion to Consider Whether Cases Should be Related (Kenny et al. v. Carrier IQ, Inc., et al. Case No. CV-11-5774-EJD Steiner v. Carrier IQ, Inc., Case No. CV-11-5802-EJD Silvera et al. v. Carrier IQ, Inc. et al., Case No. CV-11-5821-EJD Thomas et al. v. Carrier IQ, Inc. et al., Case No. CV-11-5819 LHK Pipkin et al. v. Carrier IQ, Inc. et al., Case No. CV-11-5820 EJD Patrick et al. v. Carrier IQ, Inc. et al., Case No. CV-11-5842-EJD Padilla et al. v. Carrier IQ, Inc. et al, Case No. CV-11-5975-EJD, Olivares et al. v. Carrier IQ, Inc. et al., Case No. CV-11-6151 HRL Stoltenburg et al. v. Carrier IQ, Inc. et al., ase No. CV-11-6160-PSG Medine et al. v. Carrier IQ, Inc. et al., Case No. CV-11-6178-HSG Fischer et al. v. Carrier IQ, Inc. et al., Case No. CV-11-6199-HRL Castro v. Carrier IQ, Inc. et al., Case No. CV-11-6201-PSG Gonzalez v. Carrier IQ, Inc. et al., Case No. CV-11-6202-HRL House v. Carrier IQ, Inc. et al., Case No. CV-11-6200-LHK Lavertue v. Carrier IQ, Inc. et al., Case No. CV-11-6196-MEJ Shumate v. Carrier IQ, Inc., Case No. CV-11-6281-HRL, Wadler v. Carrier IQ, Inc., Case No. CV-11-6278-PSG, Schwartz v. Carrier IQ, Inc., Case No. CV-11- 6280-HRL, Massey v. Carrier IQ, Inc. Case No. CV-11-6279-HRL) filed by Dao Phong. (Attachments: # <u>1</u> Declaration, # <u>2</u> Exhibit, # <u>3</u> Exhibit, # <u>4</u> Exhibit, # <u>5</u> Exhibit, # <u>6</u> Exhibit, # <u>7</u> Exhibit, # <u>8</u> Exhibit, # <u>9</u> Exhibit, # <u>10</u> Exhibit, # <u>11</u> Exhibit, # <u>12</u> Exhibit, # <u>13</u> Exhibit, # <u>14</u> Exhibit, # <u>15</u> Exhibit, # <u>16</u> Exhibit, # <u>17</u> Exhibit, # <u>18</u> Exhibit, # <u>19</u> Exhibit, # <u>20</u> Exhibit, # <u>21</u> Exhibit, # <u>22</u> Certificate/Proof of Service) (Punzalan, Mark) (Filed on 12/19/2011) Modified on 12/20/2011 (bw, COURT STAFF). (Entered: 12/19/2011)

ORIGINAL

Rosemary M. Rivas (State Bar No. 209147)
rrivas@finkelsteinthompson.com
Mark Punzalan (State Bar No. 247599)
mpunzalan@finkelsteinthompson.com
Danielle A. Stoumbos (State Bar No. 264784)
dstoumbos@finkelsteinthompson.com
FINKELSTEIN THOMPSON LLP
100 Bush Street, Suite 1450
San Francisco, California 94104
Telephone: (415) 398-8700
Facsimile: (415) 398-8704

Counsel for Plaintiff Dao Phong

FILED

2011 DEC 14 P 3:24

RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
N.D. CALIF. - SAN JOSE

Paid
900

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

DAO PHONG, an individual, on behalf of herself
and all others similarly situated,

CV 11-06333 Case No.

HRL

Plaintiff,

vs.

CARRIER IQ, INC.; and HTC AMERICA, INC.,

Defendants.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Dao Phong ("Plaintiff"), individually and on behalf of all others similarly situated, alleges as follows based on her counsel's investigation and her personal experience:

INTRODUCTION

1. Plaintiff brings this action for actual damages, equitable relief (including restitution, injunctive relief, and disgorgement of profits), civil penalties, and all other available relief on behalf of herself and all similarly-situated individuals and entities in the United States who, within four years of the filing of this litigation, bought a phone manufactured by Defendant HTC America, Inc. ("HTC") embedded with technology created and employed by Defendant Carrier IQ, Inc. ("Carrier IQ") (the "Class").

FAXED

4. As alleged herein, Carrier IQ's conduct violates the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.* (the "Wiretap Act"); the Stored Communications Act of 1986 ("SCA"), 18 U.S.C. §§ 2701, *et seq.*; California's Computer Crime Law ("CCCL"), Cal. Penal Code § 502, *et seq.*; and California's Unfair Competition Law, Bus. & Prof. Code § 17200, *et seq.*

THE PARTIES

5. Plaintiff Dao Phong is a citizen and resident of San Francisco, California. Plaintiff purchased an HTC Evo mobile phone manufactured by Defendant HTC and activated and maintained cellular service for this phone with Sprint. As a result of the misconduct alleged herein, Plaintiff has suffered injury in fact and has lost money or property.

6. Defendant Carrier IQ is a Delaware corporation with its principal place of business located at 1200 Villa Street, Suite 200, Mountain View, California 94041. Based on information and belief, Carrier manufactures and supports a "rootkit" software application that is installed in mobile phones by manufacturers.

7. Defendant HTC America, Inc. is a Washington corporation with its principal place of business located at 811 1st Ave., Suite 530, Seattle Washington 98104.

11

1
2
3
4
5
6
7
8
9
10
11
12
JURISDICTION

8. Pursuant to 28 U.S.C. 1331, this Court has original jurisdiction over this lawsuit arising under the Electronic Communications Privacy Act, 18 U.S.C. §§ 2511, *et seq.* This Court also has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action in which: (1) there are 100 or more members in the Plaintiff's proposed class; (2) at least some members of the proposed class have a different citizenship from one or more Defendants; and (3) the claims of the proposed class members exceed \$5,000,000 in the aggregate.

9. This Court also has personal jurisdiction because Defendants have purposefully availed themselves of the privilege of conducting business activities by advertising, contracting, and conducting services within the State of California and have generally maintained systematic and continuous business contacts with the State of California. Defendant Carrier IQ is also headquartered in California.

13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
VENUE AND INTRADISTRICT ASSIGNMENT

10. Venue is proper in the Northern District of California and in the San Jose Division, pursuant to 28 U.S.C. section 1391 subsections (b) and (c), and Civil L.R. 3-2 subsections (c) and (e). A substantial part of the events giving rise to the claims at issue in this litigation occurred in this District and Division because Defendants advertised, contracted, and conducted its services in this District and Division. Additionally, Defendant Carrier IQ is present in this Judicial District and Division and transacts business in this Judicial District and Division.

FACTUAL ALLEGATIONS

11. Carrier IQ manufactures and supports a "rootkit" software application that is installed in mobile phones by manufacturers such as HTC. According to Carrier IQ, its software application is installed on over 140 million handsets and mobile phones.

12. On its website, Carrier IQ markets itself as "the only company embedding diagnostic software in millions of subscribers' phones" and purports to track "Actionable Intelligence" on mobile phones. The Company markets itself to wireless carriers and handset manufacturers as the only company that "collects, correlates and aggregates data" in mobile phones "for near real-time system monitoring and business intelligence." Carrier IQ also states that its software performs these functions "with no visible impact to [] customers."

1 13. A recent analysis performed by computer security researcher Trevor Eckhart reveals that
2 Carrier IQ's software performs functions that are extremely intrusive to users' privacy. In a video
3 posted on YouTube, Mr. Eckhart demonstrates that Carrier IQ software can log every keystroke that the
4 user performs on her mobile phone.¹ The Eckhart video reveals that for the 140 million phones
5 embedded with the Carrier IQ software, Carriers IQ can track and collect a wealth of information by
6 tracking these keystrokes. For instance, Carrier IQ can collect information when users turn their phones
7 on and off, the phone numbers they dial, the contents of their text messages, the websites they visit, the
8 search terms they input into browsers, and their phones' locations. Carrier IQ can also collect these data
9 even when such data are supposed to be transmitted securely, *e.g.*, by HyperText Transfer Protocol over
10 Secure Socket Layer ("https").² Moreover, Carrier IQ can collect data for the location of the users'
11 phone even when the user has expressly denied location access to the phone's location.

12 14. Based on information and belief, neither Carrier IQ or HTC disclose to mobile phone
13 users that Carrier IQ software is embedded in their phone and that the software tracks and collects users'
14 actions. Based on information and belief, Carrier IQ software does not make itself readily apparent to a
15 user and does not show up in a phone's list of active processes. Even if a technologically-savvy user is
16 able to find out that Carrier IQ is running, users are not given an option to shut down the software.

17 15. Based on information and belief, once Carrier IQ collects these data from mobile phone
18 users, it provides this information to its clients, which include Handset Manufacturers such as Defendant
19 HTC. As the company states on its website, Carrier IQ "give[s] Wireless Carriers and Handset
20 Manufacturers unprecedented insight into their customers' mobile experience." Carrier IQ further states
21 that it provides "real-time data direct from [...] customers' handsets." Wireless carriers AT&T Inc., T-
22 Mobile, and Sprint (Plaintiff's wireless carrier) have admitted that Carrier IQ is present on their phones.

23 16. After news outlets reported on Eckhart's analysis of Carrier IQ, Carrier IQ issued a
24 statement denying that its software tracked usage or recorded keystrokes. This statement, however, is
25

26
27 ¹ The full video is available at http://www.youtube.com/user/TrevorEckhart#p/u/0/T17XQI_AYNo (last
visited Dec. 1, 2011).

28 ² http://en.wikipedia.org/wiki/HTTP_Secure

1 apparently not only contradicted by the Company's own website representations but by the company's
2 own patent application for its software, in which the company describes its technology as a "method for
3 collecting data at a server coupled to a communications network, comprising: transmitting to a device a
4 data collection profile... wherein the set of data relates to an end user's interaction with the device...
5 [and] wherein the interaction with the device comprises the end user's pressing of keys on the device."

6 17. According to recent news reports, after Mr. Eckhart publicly expressed concerns over
7 Carrier IQ's capabilities, Carrier IQ sent a cease-and-desist letter threatening a lawsuit. Carrier IQ
8 withdrew this threat and publicly apologized after a non-profit group intervened on Mr. Eckhart's
9 behalf. Since news reports were released regarding Carrier IQ's tracking of users' mobile phones,
10 Senator Al Franken (D-MN) also opened a probe into Carrier IQ. Senator Franken described the
11 allegations surrounding Carrier IQ as "deeply troubling" and said that Congress should act "quickly" to
12 protect consumers' privacy.

13 STATUTES OF LIMITATION

14 18. Discovery Rule. The causes of action alleged herein accrued upon discovery of Carrier
15 IQ's wrongful conduct. Because telephone users could not readily determine their phones contained
16 Carrier IQ software and Carrier took steps to actively conceal them, Plaintiff and members of the Class
17 did not discover and could not have discovered Carrier IQ's wrongful conduct through reasonable and
18 diligent investigation. Moreover, reasonable and diligent investigation into Carrier IQ's wrongful
19 conduct did not and could not reveal a factual basis for a cause of action based on Carrier IQ's
20 nondisclosure or concealment of its actions.

21 CLASS ACTION ALLEGATIONS

22 19. Plaintiff brings this lawsuit as a class action on behalf of herself and all others similarly
23 situated as members of a proposed plaintiff Class pursuant to Federal Rule of Civil Procedure 23. This
24 action satisfies the ascertainability, numerosity, commonality, typicality, adequacy, predominance and
25 superiority requirements of those provisions.

26 20. The Class is initially defined as:

27 *All persons and entities residing in the United States who purchased an HTC device embedded*
28 *with Carrier IQ software.*

b. Whether Defendants failed to disclose to Plaintiff and the Class that its software collected, tracked, and shared with third parties their private mobile phone actions;

c. Whether Defendants knew and/or were reckless in not knowing of the unlawful nature of their conduct;

d. Whether Defendants had a duty to Plaintiff and the Class to disclose their wrongful conduct;

e. Whether Defendants' conduct violated the The Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.*, the Stored Communications Act of 1986 ("SCA"), 18 U.S.C. § 2711(1), and California's Computer Crime Law, Cal. Penal Code § 502; and

f. Whether Defendants' active concealment of and/or failure to disclose the true nature of its conduct was likely to mislead or deceive, and was therefore fraudulent, within the meaning of Cal. Bus. & Prof. Code § 17200, *et seq.*

Adequacy

28. Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel with substantial experience in prosecuting consumer class actions, including actions involving privacy issues and the claims alleged herein.

29. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the Class, and have the financial resources to do so. Neither Plaintiff nor her Counsel have interests adverse to those of the Class.

Superiority

30. Absent class treatment, Plaintiff and members of the Class will continue to suffer harm and damages as a result of Defendants' unlawful and wrongful conduct.

31. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Without a class action, individual Class members would face burdensome litigation expenses, deterring them from bringing suit or adequately protecting their rights. Because of the modest economic value of the individual Class members' claims, few if any could seek their rightful legal recourse in an individual action. Absent a class action, Class members would

1 continue to incur harm without remedy, while Defendants would continue to reap the benefits of its
2 misconduct.

3 32. The consideration of common questions of fact and law will conserve judicial resources
4 and promote a fair and consistent resolution of these claims.

5 **FIRST CAUSE OF ACTION**
6 **(Violation of the Wiretap Act)**

7 33. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

8 34. The Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.* (the "Wiretap
9 Act") broadly defines an "electronic communication" as "any transfer of signs, signals, writing, images,
10 sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio,
11 electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce..."
12 18 U.S.C. § 2510(12).

13 35. Pursuant to the Wiretap Act, Defendants operate an "electronic communications service"
14 as defined in 18 U.S.C. § 2510(15).

15 36. The Wiretap Act broadly defines the contents of a communication. Pursuant to the
16 Wiretap Act, "contents" of a communication, when used with respect to any wire, oral, or electronic
17 communications, include any information concerning the substance, purport, or meaning of that
18 communication. 18 U.S.C. § 2510(8). "Contents," when used with respect to any wire or oral
19 communication, includes any information concerning the identity of the parties to such communication
20 or the existence, substance, purport, or meaning of that communication. The definition thus includes all
21 aspects of the communication itself. No aspect, including the identity of the parties, the substance of the
22 communication between them, or the fact of the communication itself, is excluded. The privacy of the
23 communication to be protected is intended to be comprehensive.

24 37. The Wiretap Act prevents an electronic communications service operator from
25 intentionally divulging the contents of any communication while in transmission on that service to any
26 person or entity other than an addressee or intended recipient of such communication. 18 U.S.C. §
27 2511(3)(a). Plaintiff and Class members are "person[s] whose ... electronic communication[s] [are]
28 disclosed... or intentionally used in violation of this chapter" within the meaning of 18 U.S.C. § 2520(a).
When users perform such functions on their phone as turning their phones on and off, dialing phone

1 numbers, sending text messages, visiting websites, users are unknowingly sending electronic
2 communications to Defendants. Users do not expect and do not consent to any disclosure of the
3 activities to their phone to Defendants or to any third parties to whom Defendants makes this
4 information available.

5 38. Based on information and belief, Defendants intentionally divulge the electronic
6 communications of mobile phone users to third parties. By divulging these communications and other
7 user information to third parties without user consent, Defendants intentionally violated 18 U.S.C. §
8 2511(3)(a).

9 39. Each incident in which Defendants divulged the electronic communications of mobile
10 phone users is a separate and distinct violation of the ECPA. Plaintiff and members of the Class
11 therefore seek remedies as provided for by 18 U.S.C. § 2520, including such preliminary and other
12 equitable or declaratory relief as may be appropriate, damages consistent with subsection (c) of that
13 section to be proven at trial, punitive damages to be proven at trial, and attorneys' fees and other
14 litigation costs reasonably incurred.

15 40. Plaintiff and the Class, pursuant to 18 U.S.C. § 2520(2), are entitled to preliminary,
16 equitable, and declaratory relief, in addition to statutory damages of the greater of \$10,000 or \$100 a day
17 for each day of violation, actual and punitive damages, reasonable attorneys' fees, and Defendants'
18 profits obtained from the violations described herein.

19 SECOND CAUSE OF ACTION

20 (Violations of the Stored Communications Act)

21 41. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

22 42. The Stored Communications Act of 1986 ("SCA") incorporates the Wiretap Act's
23 definition of an "electronic communication service." 18 U.S.C. § 2711(1). As set forth above,
24 Defendants are electronic communications service providers within the meaning of the ECPA and is
25 therefore also subject to the restrictions contained in the SCA governing electronic communications
26 service providers. The SCA also incorporates the Wiretap Act's broad definition of "electronic
27 communication" and "electronic storage." 18 U.S.C. § 2711(1). Pursuant to the Wiretap Act and the
28 SCA, "electronic storage" means any "temporary storage of a wire or electronic communication

1 incidental to the electronic transmission thereof.” 18 U.S.C. § 2510(17)(A). This type of electronic
2 storage includes communications in intermediate electronic storage that have not yet been delivered to
3 their intended recipient.

4 43. The SCA prohibits any electronic communications service provider from divulging to
5 any person or entity the contents of a communication while in electronic storage by that service. 18
6 U.S.C. § 2702(a)(1). Based on information and belief, Defendants provide this information to third
7 parties. When users perform functions on their phones such as making a phone call, sending a text
8 message, or browsing the internet, users do not expect, intend and consent for Carrier IQ to collect and
9 track this information or pass along the communications to a third party as a handset manufacturer.
10 Based on information and belief, Defendants provide users’ information regarding electronic
11 communications to third parties in violation of 18 U.S.C. § 2702(a)(1). By disclosing these
12 communications, Defendants violated 18 U.S.C. § 2702(a)(1).

13 44. The SCA definition of “electronic storage” also includes “storage of [a wire or electronic]
14 communication by an electronic communication service for purposes of backup protection of such
15 communication.” 18 U.S.C. § 2510(17)(B). The information that Defendants collect from users via
16 electronic communications are electronically stored by Defendants for backup purposes.

17 45. The SCA, at 18 U.S.C. § 2702(a)(2), provides that “a person or entity providing a remote
18 communication service to the public shall not knowingly divulge to any person or entity the contents of
19 any communication which is carrier or maintained on that service (A) on behalf of, and received by
20 means of electronic transmission...a subscriber or customer of such service; (B) solely for the purpose
21 of providing storage...to such subscriber or customer, if the provider is not authorized to access the
22 contents of any such communications for purposes of providing any services other than storage or
23 computer processing.”

24 46. Plaintiff and Class members are “person[s] aggrieved by [a] violation of [the SCA] in
25 which the conduct constituting the violation is engaged in with a knowing or intentional state or
26 mind...” within the meaning of 18 U.S.C. § 2707(a).

27 //

28 //

49. Plaintiff and the Class, pursuant to 18 U.S.C. § 2707(c), are entitled to preliminary, equitable, and declaratory relief, in addition to statutory damages of no less than \$1,000 per violation, actual and punitive damages, reasonable attorneys' fees, and Defendants' profits obtained from the violations described herein.

THIRD CAUSE OF ACTION

Violation of California's Computer Crime Law ("CCCL"), Cal. Penal Code § 502

50. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

51. Defendants knowingly accessed and without permission used any data, computer, computer system, or computer network in order to execute a scheme or artifice to deceive and/or to wrongfully control or obtain money, property, or data in violation of Cal. Penal Code § 502(c)(1).

52. Defendants did so by accessing and sharing with wireless carriers and handset manufacturers the mobile phone actions of Plaintiff and Class members in order to deceive and/or to wrongfully profit by collecting, tracking and disclosing users' information.

53. Defendants knowingly accessed and without permission took, copied, or made use of Plaintiff and Class members' information regarding actions performed on their mobile phones in violation of § 502(c)(2).

54. Defendants knowingly and without permission used or caused to be used computer services by impermissibly accessing, collecting, and transmitting Plaintiffs' and Class members' personal information in violation of § 502(c)(3).

1 55. Defendants knowingly and without permission provided or assisted in providing a means
2 of accessing a computer, computer system, or computer network by creating a system that allowed third
3 parties to impermissibly access, collect, and transmit Plaintiffs' and Class members' private mobile
4 phone actions in violation of § 502(c)(6).

5 56. Defendants knowingly and without permission accessed or caused to be accessed
6 Plaintiff and Class members' computers and/or computer networks by impermissibly divulging
7 Plaintiffs' and Class members' personal information to advertisers in violation of § 502(c)(7).
8 Defendants knowingly and without permission introduced a computer contaminant, as defined in §
9 502(b)(10), by introducing computer instructions designed to record or transmit to third parties Plaintiff
10 and the Class' private actions performed on their phones on Defendants' computer networks without the
11 intent or permission of Plaintiff or the Class in violation of § 502(c)(8). These instructions usurped the
12 normal operations of the relevant computers, which by normal operation would not transmit the private
13 mobile phone information of Plaintiff and/or the Class members.
14

15 57. As a direct and proximate result of Defendants' violation of § 502, Defendants caused
16 loss to Plaintiff and the Class members in an amount to be proven at trial. Plaintiff and the Class are
17 entitled to the recovery of attorneys' fees pursuant to § 502(e).

18 58. Plaintiff and Class members have also suffered irreparable injury as a result of
19 Defendants' unlawful conduct, including the collection and sharing of their personal mobile phone
20 information. Additionally, because the stolen information cannot be returned, the harm from this breach
21 is ongoing and compounding. Accordingly, Plaintiff and the Class have no adequate remedy at law,
22 entitling them to injunctive relief.

23 **FOURTH CAUSE OF ACTION**

24 **Violation of California's Unfair Competition Law**
25 **Cal. Bus. & Prof. Code § 17200, *et seq.***

26 59. Plaintiff incorporates the foregoing allegations as if fully set forth herein. California
27 Business & Professions Code § 17200, *et seq.* ("UCL"), prohibits acts of "unfair competition." The
28 UCL defines unfair competition as any unlawful, unfair, or fraudulent business act or practice. Thus,

1 under the UCL, there are three categories of unfair competition: conduct that is unlawful, conduct that is
2 unfair, and conduct that is fraudulent.

3 60. Defendants violated the UCL by engaging in conduct that violated each of the three
4 prongs of the statute.

5 61. Defendants' practice of, among other things, collecting and tracking keystrokes by users
6 and disclosing them to third parties is unlawful because it violates, among other things, the Wiretap Act,
7 the SCA, and CCCL, as alleged above.

8 62. Defendants engaged in unfair business practices by, among other things:

9 g. Engaging in conduct that causes a substantial injury to consumers, specifically by
10 disclosing their private mobile information to third parties. Defendants' practices are not outweighed by
11 any countervailing benefits to consumers or to competition. Consumers could not have reasonably
12 avoided this injury.

13 h. Engaging in conduct that is immoral, unethical, oppressive, unscrupulous, or
14 substantially injurious to Plaintiff and other members of the Class; and

15 i. Engaging in conduct that undermines or violates the stated policies underlying the
16 SCA, Wiretap Act, and CCCL.

17 63. Defendants engaged in fraudulent business practices by concealing and/or failing to
18 disclose the true nature and characteristics of its collection, tracking, and disclosure of private mobile
19 phone information. Defendants had a duty to disclose such information by virtue of their exclusive
20 knowledge, among other things.

21 64. As a direct and proximate result of Defendants' violation of Cal. Bus. & Prof. Code §
22 17200, *et seq.*, Plaintiff suffered injury in fact and lost money or property, in that she paid money to
23 purchase her phone. Plaintiff and the Class members are entitled to monetary relief, including
24 restitution of all amounts that Defendants billed and collected, as well as attorneys fees under Cal. Code
25 of Civ. P. § 1021.5. Further, as a result of Defendants' violation of the UCL, Defendants have been
26 unjustly enriched and should be required to make restitution to Plaintiff and the Class or to disgorge its
27 ill-gotten profits pursuant to Cal. Bus. & Prof. Code § 17203.
28

65. Plaintiff and the Class members are entitled to equitable relief, including declaratory relief and a permanent injunction enjoining Defendants from continuing their unlawful, unfair, and fraudulent billing practices.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for relief and judgment against Defendant as follows:

- A. Certifying the Class pursuant to Rule 23 of the Federal Rules of Civil Procedure, certifying Plaintiff as representative of the Class, and designating her counsel as counsel for the Class;
- B. Awarding Plaintiff and the Class compensatory damages, in an amount exceeding \$5,000,000, to be determined by proof;
- C. Awarding Plaintiff and the Class statutory damages;
- D. Requiring Defendants to make restitution and/or disgorgement;
- E. Imposition of a constructive trust for the benefit of Plaintiff and the Class on all monies wrongfully taken or received by Defendants;
- F. Equitable and declaratory relief, and an order enjoining Defendants from continuing to engage in the wrongful acts and practices alleged herein;
- G. Awarding Plaintiff and the Class the costs of prosecuting this action, including expert witness fees;
- H. Awarding Plaintiff and the Class reasonable attorney's fees;
- I. Awarding pre-judgment and post-judgment interest; and
- J. Granting other relief as this Court may deem just and proper under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury of all claims so triable.

DATED: December 14, 2011

FINKELSTEIN THOMPSON LLP

By: 

Mark Punzalan

Rosemary M. Rivas
Danielle A. Stoumbos
100 Bush Street, Suite 1450
San Francisco, California 94104
Telephone: (415) 398-8700
Facsimile: (415) 398-8704

Counsel for Plaintiff Dao Phong

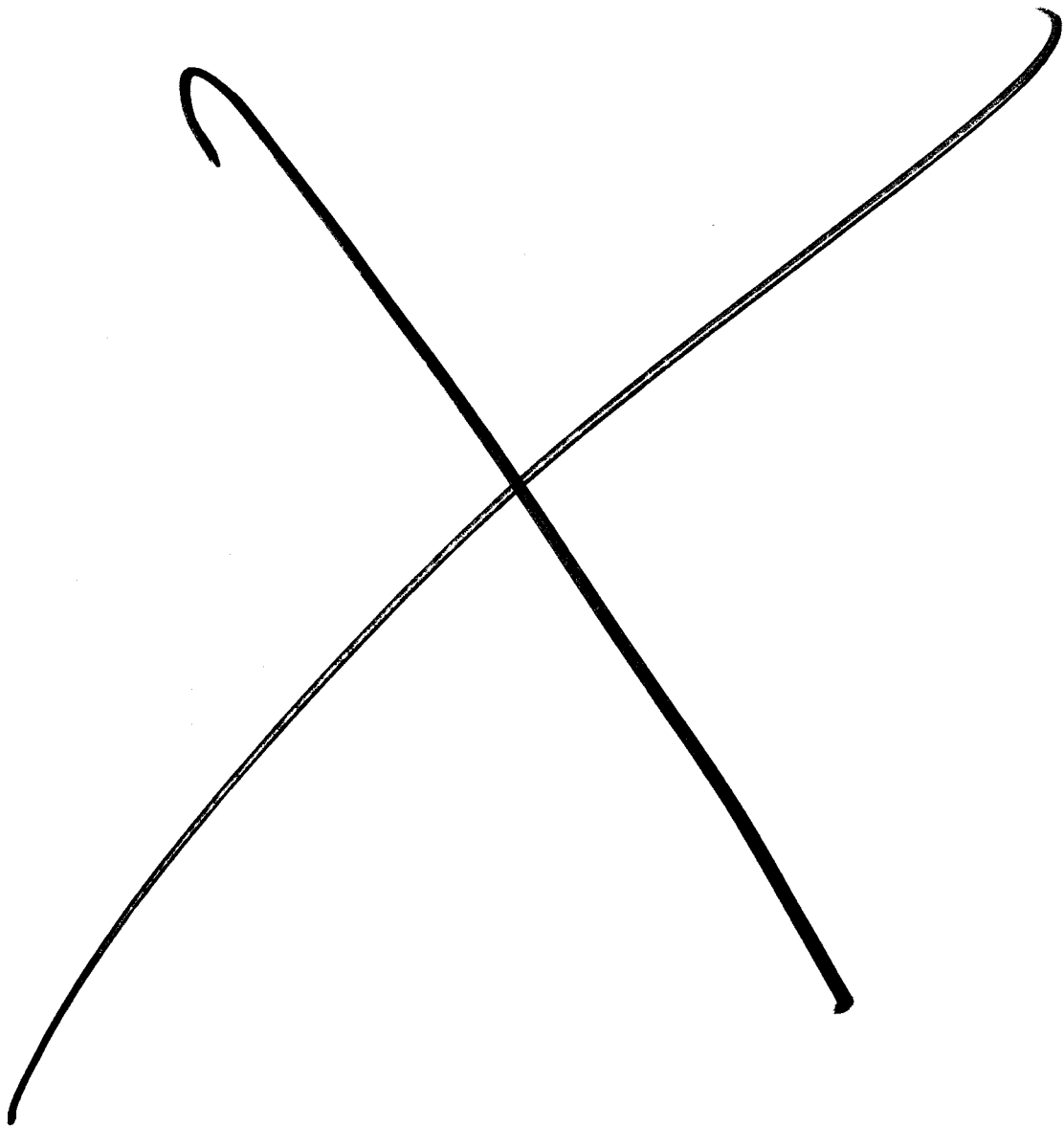


Exhibit 4:

Siegel v. Carrier IQ, Inc., et al.

MASON

**United States District Court
Northern District of Illinois – CM/ECF LIVE, Ver 4.2 (Chicago)
CIVIL DOCKET FOR CASE #: 1:11-cv-08791**

Siegel v. Carrier IQ, Inc. et al
Assigned to: Honorable Ronald A. Guzman
Cause: 28:1331 Federal Question

Date Filed: 12/12/2011
Jury Demand: Plaintiff
Nature of Suit: 890 Other Statutory
Actions
Jurisdiction: Federal Question

Plaintiff

Michael Siegel
*individually and on behalf of all others
similarly situated*

represented by **Larry D. Drury**
Larry D. Drury, Ltd.
100 N. LaSalle St.
Suite 1010
Chicago, IL 60602
(312) 346-7950
Email: ldrurylaw@aol.com
ATTORNEY TO BE NOTICED

V.

Defendant

Carrier IQ, Inc.
a California Corporation

Defendant

Sprint-Nextel Corporation
a Kansas Corporation

Defendant

Samsung Electronics America Inc
a New York Corporation

Defendant

HTC America, Inc.
a Texas Corporation

Date Filed	#	Docket Text
12/12/2011	<u>1</u>	COMPLAINT filed by Michael Siegel; Jury Demand. Filing fee \$ 350, receipt number 0752-6647654.(Drury, Larry) (Entered: 12/12/2011)
12/12/2011	<u>2</u>	CIVIL Cover Sheet (Drury, Larry) (Entered: 12/12/2011)
12/12/2011	<u>3</u>	ATTORNEY Appearance for Plaintiff Michael Siegel by Larry D. Drury (Drury, Larry) (Entered: 12/12/2011)
12/12/2011		CASE ASSIGNED to the Honorable Ronald A. Guzman. Designated as Magistrate Judge the Honorable Michael T. Mason. (ef,) (Entered: 12/12/2011)

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION**

MICHAEL SIEGEL, individually and on
behalf of all others similarly situated,

Plaintiffs,

v.

CARRIER IQ, INC., a California Corporation,
SPRINT-NEXTEL CORPORATION, a Kansas
Corporation, SAMSUNG ELECTRONICS
AMERICA, INC., a New York Corporation, and
HTC AMERICA, INC., a Texas Corporation,

Defendants.

Case No. 11-cv-8791

Jury Trial Demanded

CLASS ACTION COMPLAINT

NOW COMES PLAINTIFF, Michael Siegel, by and through his attorneys, Larry D. Drury, Ltd., and complains of the Defendants, Carrier IQ, Inc., Sprint-Nextel Corporation, Samsung Electronics America, Inc., and HTC America, Inc., as follows:

Nature of the Action

1. This case arises from the Defendants' creation, use and implementation of software hidden in consumers' cellular devices that surreptitiously logs and transmits especially sensitive information from the device to the mobile phone carriers, without the knowledge or consent of the consumer and in violation of federal and state privacy laws.

Jurisdiction & Venue

2. This Court has personal jurisdiction over all parties because all Defendants conduct business in this District, and the Plaintiff resides in this District. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §1331 because this action arises under federal statutes, i.e., the Federal Wiretap Act, 18 U.S.C. §2511, the Stored Electronic Communications Act, 18 U.S.C.

§2701 and the Computer Fraud and Abuse Act, 18 U.S.C. §1020, and pursuant to 28 U.S.C. §1332(d) because the amount in controversy exceeds \$5,000,000.00.

3. Venue is proper in this District because all conduct business in this District, and the claims from which this lawsuit arises occurred within this District.

Parties

4. Plaintiff, Michael Siegel (hereinafter "Plaintiff"), is an individual who resides in the County of Lake, State of Illinois.

5. Carrier IQ, Inc., (hereinafter "Carrier IQ"), is a California corporation with its principal place of business in Mountain View, CA.

6. Sprint-Nextel Corporation (hereinafter "Sprint") is a Kansas Corporation with its principal place of business in Overland Park, KS.

7. Samsung Electronics America, Inc., (hereinafter "Samsung"), is a New York Corporation with its principal place of business in Ridgefield Park, NJ.

8. HTC America, Inc., (hereinafter "HTC"), is a Texas corporation with its principal place of business in Bellevue, WA.

Facts Common to All Counts

9. Carrier IQ developed, marketed, and sold 'rootkit'¹ software (hereinafter "Spy Software") designed to collect and/or record data from consumers' mobile cellular devices. Its software is designed to provide wireless carriers and device makers with access to the mobile device while actively hiding its presence from the device's user.

¹ Rootkit software is software that enables continued privileged access to a computer while actively hiding its presence from administrators by subverting standard operating system functionality or other applications. Once a Rootkit is installed, it allows an attacker to mask the ongoing intrusion and maintain privileged access to the computer by circumventing normal authentication and authorization mechanisms.

10. Carrier IQ claims to be the market leader in “mobile service intelligence” rootkit software.

11. The Defendant carriers and device manufacturers, Sprint, Samsung and HTC, pre-install Carrier IQ’s Spy Software on cellular mobile devices used by its consumers. The Spy Software is a hard-to-detect and hard-to-remove application that conducts surreptitious and highly intrusive tracking of personal data including, but not limited to, a user’s location, Web browsing history and habits, videos watched, text messages read, keys typed (known as ‘keystroke logging’), and all other activities of the user.

12. The Defendants have designed and installed the Spy Software to run when the phone is switched on, and to continue to ‘spy’ on the user until the phone is switched off.

13. The United States Senate Committee on the Judiciary has labeled the Defendants’ use of the Spy Software as “a potentially very serious matter” that “may violate federal privacy laws, including the Electronic Communications Privacy Act and the Computer Fraud and Abuse Act”.

14. The Plaintiff is a customer of Sprint and a user of phones manufactured by HTC and Samsung which, on information and belief, include the Spy Software.

15. The Defendants undertook no steps to inform or otherwise notify the Plaintiff and Class that:

- a. his HTC and Samsung phones had Carrier IQ’s Spy Software pre-installed and operational;
- b. his every movement was being collected, tracked, recorded, monitored and transmitted; and

- c. his use of the HTC and Samsung phones, including Web history, private text messages, keys typed and videos watched, was being collected, tracked, recorded, monitored and transmitted.

16. The Plaintiff and Class did not consent to or otherwise authorize the Defendants to engage in the aforesaid conduct, to pre-install and operate Spy Software on their mobile devices, or to monitor, track, record and transmit their movements and private use data.

17. As a result of the Defendants' aforesaid conduct, the Plaintiff and Class have suffered damages including, but not limited to, the cost of and service charges for the use and operation of said phones.

Facts Common to the Class

18. The Plaintiff brings these claims on behalf of himself and a class² of similarly situated individuals who, from 2001 to the date of judgment in this case, had a wireless contract for cellular service with Sprint, and who used at least one cell phone manufactured and/or distributed by at least one of the Defendant manufacturers, HTC and/or Samsung, that contained Carrier IQ's software.

19. The Class is comprised of thousands of class members, making the joinder of such cases impracticable.

20. Disposition of the claims as a class action will provide substantial benefits to the parties, the class, and the Court, including ensuring efficient and uniform proceedings.

² Excluded from the Class are the Defendants, any and all of the Defendants' agents, subsidiaries, parents, successors, predecessors, and/or any entity which the Defendants or any of its parents or subsidiaries have a controlling interest in and their current and former employees, officers, and directors, any Judge to whom this case is assigned and that Judge's immediate family, any and all persons who execute and file a timely request for exclusion, and the legal representatives, successors, or assigns of any such excluded person.

21. Certification of this case as a class action will reduce the possibility of repetitious litigation involving, potentially, thousands of class members.

22. The rights of each member of the Class were violated in a similar fashion based upon the Defendants' practice and policy of using pre-installed and activated Spy Software to surreptitiously and intrusively collect, track, record, monitor and transmit their consumers' personal data including, but not limited to, the user's location, Web browsing history and habits, videos watched, text messages read, keys typed, and all other activities of the user

23. Plaintiff is a member of the class he seeks to represent, and will fairly and adequately represent and protect the interests of the Class in that Plaintiff has no interest antagonistic to or that irreconcilably conflicts with those of any other members of the Class.

24. Plaintiff has retained counsel who are highly competent and experienced in the prosecution of class-action litigation.

25. A class action is superior to all other available methods for the fair and efficient adjudication of Plaintiff's and the other Class members' claims.

26. Questions of law and fact common to the Class exist and predominate over any questions that may affect individual members, including but not limited to:

- a. Whether Sprint concealed from its consumers and/or notified its consumers of the presence of pre-installed Carrier IQ Spy Software on their mobile cellular devices;
- b. Whether HTC and Samsung concealed from its consumers and/or notified its consumers of the presence of the pre-installed Carrier IQ Spy Software on their mobile cellular devices;

- c. Whether the Defendants collected, tracked, recorded, monitored and/or transmitted their consumers' data without their consumers' consent or knowledge;
- d. Whether the Defendants' conduct violated the Federal Wiretap Act, 18 U.S.C. §2511;
- e. Whether the Defendants' conduct violated the Stored Electronic Communications Act, 18 U.S.C. §2701;
- f. Whether the Defendants' conduct violated the Computer Fraud & Abuse Act, 18 U.S.C. §1030.
- g. Whether the Defendants' conduct rises to the level of an invasion of privacy and/or misappropriation of private information; and
- h. Whether the Defendants committed a trespass to chattel by their aforesaid conduct.

Count I

Violation of the Federal Wiretap Act, 18 U.S.C. §2511

27. Plaintiff and the Class re-allege and incorporate by reference the allegations contained in ¶¶1-26 above, as if fully restated in this Count I.

28. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, prohibits the willful interception of any wire, oral, or electronic communication, and provides a private right of action to any person whose wire, oral or electronic communication is intercepted. 18 U.S.C. §2520(a).

29. Defendants installed Carrier IQ's Spy Software on Plaintiff's and the Class' mobile cellular devices for purposes of intercepting records of their users' phone communications and locations, and did so without the knowledge or consent of the Plaintiff and Class members.

30. The data that the Defendants intentionally intercepted are "communications" within the meaning of the Wiretap Act.

31. The Defendants' placement of the Spy Software on users' phones, and the Defendants' interception of the users' personal electronic communications, were done intentionally.

32. Plaintiffs are 'persons' whose electronic communications were intercepted within the meaning of the Wiretap Act. 18 U.S.C. §2520.

33. Pursuant to the Wiretap Act, Plaintiff and the Class are entitled to preliminary, equitable and declaratory relief, in addition to statutory damages of the greater of \$10,000.00 or \$100/day for each day of the violation, plus actual and punitive damages, reasonable attorneys' fees, and disgorgement of any profits earned by the Defendants as a result of the above described violation.

Count II

Violation of the Stored Electronic Communications Act, 18 U.S.C. §2701

34. Plaintiff and the Class re-allege and incorporate by reference the allegations contained in ¶¶1-33 above, as if fully restated in this Count II.

35. The Stored Electronic Communications Act ("SECA") permits a cause of action to be brought against a person who intentionally accesses without authorization a facility through which an electronic communication is provided, or who intentionally exceeds an authorization to access that facility, and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in store in such a system. 18 U.S.C. §2701.

36. The SECA defines “electronic storage” as “any temporary, immediate storage of a wire or electronic communication incidental to the electronic transmission thereof.”

37. The Defendants intentionally placed software on users’ phones that accessed their electronically stored communications without authorization, and in doing so violated the SECA.

38. The Plaintiff and Class members were harmed by the Defendants’ violations, and are entitled to statutory, actual and compensatory damages, injunctive relief, punitive damages, and reasonable attorneys’ fees.

Count III
Violation of The Computer Fraud and Abuse Act, 18 U.S.C. §1030

39. Plaintiff and the Class re-allege and incorporate by reference the allegations contained in ¶¶1-38 above, as if fully restated in this Count III.

40. Plaintiff’s and the Class’ cellular phones are “computers” within the meaning of the Computer Fraud & Abuse Act (CFAA), and are used for interstate commerce or communication.

41. The Defendants intentionally and knowingly accessed the Plaintiff’s and Class’ cellular phones without authorization or by exceeding authorized access to said phones, and in doing so obtained information from a protected “computer” within the meaning of the CFAA.

42. The Defendants’ violated the privacy rights of the Plaintiff and the Class by their aforesaid conduct.

43. In committing the aforesaid acts, the Defendants violated the CFAA and caused Plaintiff and the Class to suffer irreparable injury. Unless retrained from doing so, the Defendants may continue to commit such acts.

44. Should the Court find that the Plaintiff’s and Class’ remedies at law are not adequate to compensate them for these wrongs, the Court may award injunctive relief as provided for by 18 U.S.C. §1030(g).

Count IV

Invasion of Privacy and Misappropriation of Confidential Information

45. Plaintiff re-alleges paragraphs 1 through 44 of this Complaint as if fully set forth herein in this Count IV.

46. Plaintiff and the Class have a legally protected privacy interest in their confidential and private communications and data, and have a reasonable expectation of privacy in such information. This right of privacy includes the right to not have their confidential and private communications and data collected, tracked, recorded, monitored and/or transmitted to some third-party or other unintended recipient.

47. As alleged herein, Defendants collected, tracked, recorded, monitored and/or transmitted confidential and private communications and data of the Plaintiff and the Class without their knowledge, authorization or consent. This unauthorized collecting, tracking, recording, monitoring and transmission of such private facts and information is one that is highly offensive or objectionable to a reasonable person of ordinary sensibilities. Moreover, the collecting, tracking, recording, monitoring and transmission of such private facts and information, as alleged herein, does not include information which is of a legitimate public concern.

48. As a result of the Defendants' unlawful conduct, as alleged herein, the privacy rights of Plaintiff and the Class have been violated, and Plaintiff and the Class have been harmed as a result thereof.

Count V
Trespass To Chattel

49. Plaintiff re-alleges paragraphs 1 through 48 of this Complaint as if fully set forth herein in this Count V.

50. The Defendants' placed its Spy Software onto the mobile cellular devices of the Plaintiff and Class for purposes of collecting, tracking, recording, monitoring and transmitting their private information as alleged above.

51. The Spy Software was pre-installed and made to be operational and functioning without any notice to the Plaintiff and Class, and without the Plaintiff's and Class' consent.

52. The Defendants' conduct constitutes a 'taking' of the Plaintiff's and Class' mobile cellular devices and/or of the Plaintiff's and Class' private and confidential information contained thereon.

Prayer for Relief

WHEREFORE, Plaintiff prays that this Court:

- a. Certify this matter as a class action and appoint Plaintiff as Class Representative, and designate Plaintiff's counsel as class counsel;
- b. Declare that the Defendants' conduct is in violation of the Federal Wiretap Act, 18 U.S.C. §2511;
- c. Declare that the Defendants' conduct is in violation of the Stored Electronic Communications Act, 18 U.S.C. §2701;
- d. Declare that the Defendants' conduct is in violation of the Computer Fraud and Abuse Act, 18 U.S.C. §1030;
- e. Find that the Defendants invaded the Plaintiff's and Class' privacy and misappropriated their private information and data;

- f. Find that the Defendants committed a trespass to chattel;
- g. Require the Defendants to pay actual, compensatory, and punitive damages for their conduct as alleged herein;
- h. Award reasonable attorneys' fees and costs; and
- i. Grant such other relief as this Court deems just and appropriate.

Plaintiff demands trial by jury on all counts.

Dated: December 12, 2011

Michael Siegel, individually and on behalf of all
others similarly situated,

s/ Larry D. Drury

Larry D. Drury
Attorney for the Plaintiff and the Class

Larry D. Drury
James R. Rowe
Larry D. Drury, Ltd.
100 N. LaSalle St., Ste. 1010
Chicago, IL 60602
(312) 346-7950
0681024

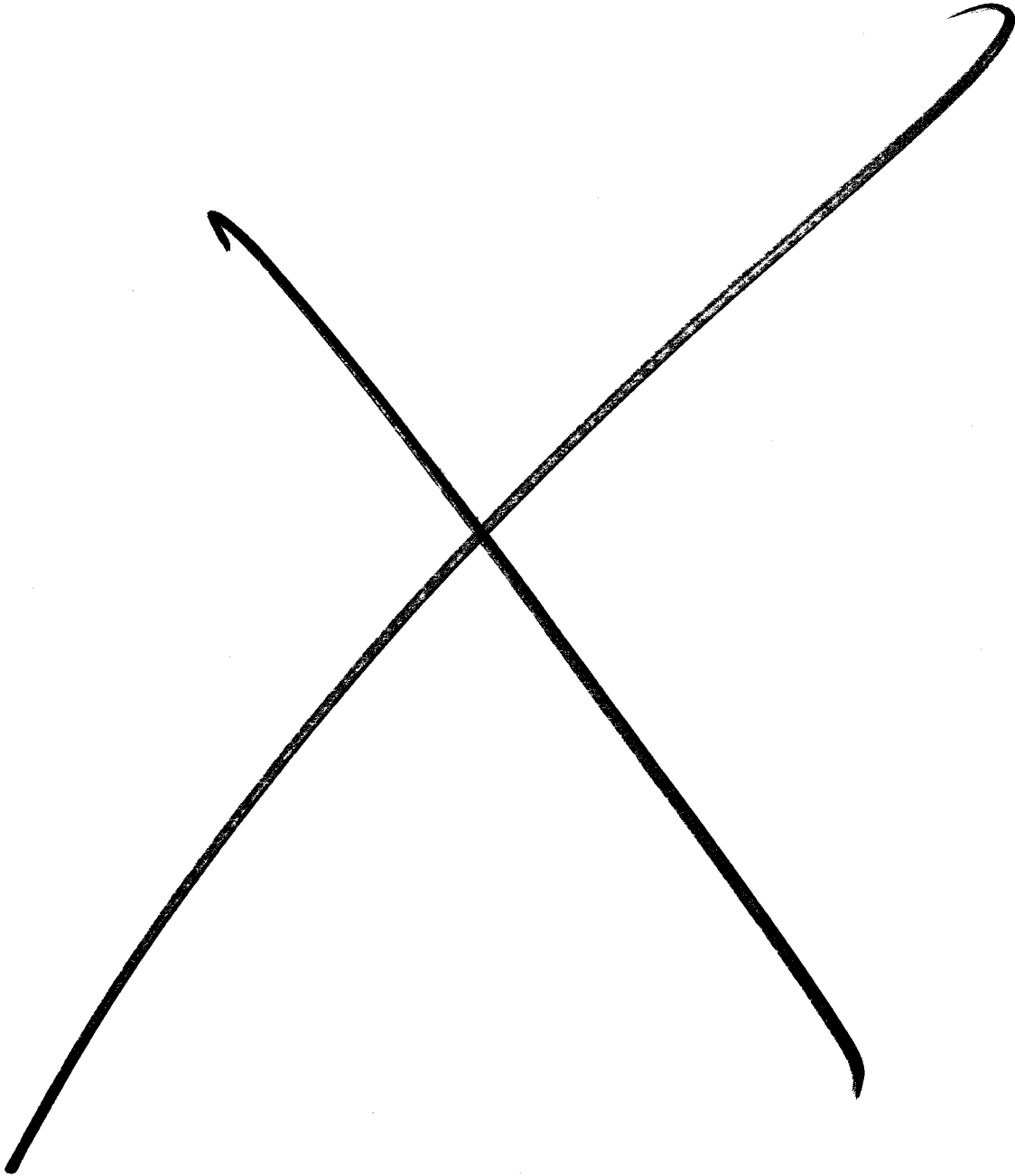


Exhibit 5:

Cerrone v. Carrier IQ, Inc., et al.

**U.S. District Court
Eastern District of New York (Brooklyn)
CIVIL DOCKET FOR CASE #: 1:11-cv-05994-RRM-JMA**

Cerrone v. Carrier IQ, Inc. et al
Assigned to: Judge Roslynn R. Mauskopf
Referred to: Magistrate Judge Joan M. Azrack
Cause: 28:1331 Fed. Question

Date Filed: 12/08/2011
Jury Demand: Plaintiff
Nature of Suit: 440 Civil Rights: Other
Jurisdiction: Federal Question

Plaintiff

Kristina Cerrone
*individually and on behalf of all others
similarly situated*

represented by **Michael M. Weinkowitz**
Levin Fishbein Sedran & Berman
510 Walnut Street
Suite 500
Philadelphia, PA 19106
215-592-1500
Fax: 215-592-4663
Email: mweinkowitz@lfsblaw.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

V.

Defendant

Carrier IQ, Inc.

Defendant

HTC, Inc.

Defendant

HTC America, Inc.

Date Filed	#	Docket Text
12/08/2011	<u>1</u>	COMPLAINT against All Defendants Disclosure Statement on Civil Cover Sheet completed -no., filed by Kristina Cerrone. (Attachments: # <u>1</u> Civil Cover Sheet) (Bowens, Priscilla) (Entered: 12/13/2011)
12/08/2011		FILING FEE: \$ 350, receipt number 4653037324 (Bowens, Priscilla) (Entered: 12/13/2011)
12/08/2011		Summons Issued as to All Defendants. (Bowens, Priscilla) (Entered: 12/13/2011)
12/16/2011		SCHEDULING ORDER: An Initial Conference will be held in Courtroom 6E, 225 Cadman Plaza East, before Magistrate Judge Azrack on Frebruary 21, 2012, at 1:00 PM. All counsel must be present and are advised to review Judge Azrack's revised Individual Rules, which are available on the District Court's web site, prior to the conference. <u>Plaintiff's counsel is directed to confirm with defendant's counsel that all necessary participants are aware of this conference.</u> Any request for an adjournment must be made in the form of a letter motion filed on ECF at least forty-eight (48) hours before the scheduled conference and must indicate which parties consent to the adjournment. Ordered by Magistrate Judge Joan M. Azrack on 12/16/2011. (Beauchamp, Peter) (Entered: 12/16/2011)

PRESS

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK**

**KRISTINA CERRONE, individually, and
on behalf of all others similarly situated**

Plaintiff,

vs.

**CARRIER IQ, INC., HTC, INC., and HTC
AMERICA, INC.,**

Defendants.

Case No.

JURY TRIAL DEMANDED

11-5994

IN CLERK'S OFFICE
U.S. DISTRICT COURT E.D.N.Y.

★ DEC - 8 2011

MAILED

BROOKLYN OFFICE

AZRACK, N.J.

COMPLAINT

COMES NOW Plaintiff, individually, and on behalf of all others similarly situated, by and through their undersigned counsel, on information and belief, and for their Complaint against Defendants Carrier IQ, Inc. and HTC state as follows:

1. Defendants have unlawfully intercepted private electronic communications emanating from private mobile phones, handsets and smart phones. This practice violates Federal Law.

PARTIES, JURISDICTION AND VENUE

2. Kristina Cerrone is a natural person and citizen and resident of the State of New York.

3. All references to "Plaintiff(s)" throughout this Complaint are made on behalf of the named Plaintiff(s) and the proposed plaintiff class(es), and vice versa.

4. This Court has subject matter jurisdiction over this action and Defendants pursuant to 28 U.S.C. § 1331 because this action arises under federal statutes, namely the Federal Wiretap Act, 18 U.S.C. § 2511, *et seq.* (the "Wiretap Act").

5. Diversity jurisdiction also arises under CAFA, 28 U.S.C. § 1332(d).

6. The amount in controversy in this action, as defined by 28 U.S.C. § 1332(d)(6), exceeds \$5,000,000 exclusive of costs and interest.

7. Defendant, Carrier IQ, Inc. (hereinafter referred to as "CIQ") is a citizen of California as defined by 28 U.S.C. § 1332(c) with its principal place of business in California.

8. Defendants HTC, Inc. and HTC America (collectively referred to as "HTC") are citizens of Washington, with their principle place of business in Bellevue, Washington.

9. Defendants are residents of the Eastern District of New York as they have ongoing and systematic contacts with residents of the Eastern District of New York. Defendants have, at all material times, conducted business in the Eastern District of New York. Moreover, Defendants have sufficient minimum contacts with the State of New York such that the assumption of jurisdiction will not offend traditional notions of fair play and substantial justice.

10. When reference in this Complaint is made to any act or omission of Defendants, it should be deemed to mean that the officers, directors, agents, employees, or representatives of Defendants committed or authorized such act or omission, or failed to adequately supervise or properly control or direct their employees while engaged in the

management, direction, operation, or control of the affairs of Defendants, and did so while acting within the scope of their employment or agency.

STATEMENT OF FACTS

11. Defendant, CIQ is the leading provider of mobile services intelligence solutions to the wireless industry.

12. Defendant, CIQ claims on their website: "As the only embedded analytics company to support millions of devices simultaneously, we give wireless carriers and handset manufacturers unprecedented insight into their customers' mobile experience."

13. Defendant, CIQ uses software in mobile phones to measure performance and user experience with no visible notice or impact to the user.

14. Defendant, CIQ's data processing center collects the data for near real-time monitoring and intelligence.

15. Defendant, CIQ is the only company in the industry embedding diagnostic software in millions of mobile phones, having done so in over 130 million phones globally.

16. Defendant CIQ states on their website "Identify exactly how your customers interact with services and which ones they use. See which content they consume, EVEN OFFLINE" (caps added).

17. They further state on their website that their software answers business critical questions including "How do users respond to mobile advertising."

18. Their website further states that their software features include "View application and device feature usage, such as camera, music, messaging, browser and TV."

19. Defendant CIQ further states that their services give "uniquely powerful insight into mobile service quality and USER BEHAVIOR" (caps added), allowing the customer to "identify new business opportunities."

20. Defendant further states that their software "uses data directly from the mobile phone itself to give a precise view of how users interact with both their phones and the services delivered through them, EVEN IF THE PHONE IS NOT COMMUNICATING WITH THE NETWORK....Identify exactly how your customers interact with services and which ones they use. SEE WHICH CONTENT THEY CONSUME, EVEN OFFLINE" (caps added).

21. Privacy concerns surrounding Carrier IQ initially arose after Trevor Eckhart, a security researcher, posted a video which seemingly demonstrated Carrier IQ's keystroke logging, even offline.

22. Carrier IQ's patent application #20110106942 contains claims regarding the collection of keystroke data, describing their product as a "method of collecting data...wherein the data relates to an end user's interaction with the device...wherein the interaction with the device comprises the end user's pressing of keys on the device."

23. A CIQ representative has been quoted in response to the privacy concerns as follows:

Andrew Coward-Chief marketing officer

"We're as surprised as anybody to see all that information flowing. It raises a lot of questions for the industry-and not (only) for Carrier IQ." CARRIER IQ: WE'RE AS SURPRISED AS YOU: CNNMoney.com 12/02/11

"We do recognize the power and value of this data. We're very aware that this information is sensitive. It's a treasure trove....We're seeing URLs and we can capture that information." CARRIER IQ ADMITS HOLDING TREASURE TROVE OF CONSUMER DATA, BUT NOT KEYSTROKES: Wired.com 12/02/2011

In an interview with Wired.com Coward said "probably yes" when asked whether Carrier IQ could read mobile users' text messages. CRITICS LINE UP TO BASH MAKER OF SECRET PHONE-MONITORING SOFTWARE: Wired.com 12/01/11

24. Defendant, CIQ captures and records keystroke data entered on the mobile device and other data.

25. Defendant, HTC produces mobile phones and handsets, including "Android" smart phones.

26. The CIQ software is embedded in HTC Android phones.

27. The information collected by CIQ is transmitted to various service providers, including Sprint and AT&T.

28. Until August 2011, Plaintiff owned an HTC Android phone. Plaintiff used her phone to electronically send over her cellular phone network various types of private data. This data was not readily accessible to the general public. She did not know that Defendants were surreptitiously monitoring and collecting this data, nor did she give them permission to do so.

29. Defendants intercepted, recorded and collected information concerning the substance, purport, or meaning of the electronic communications transmitted without the authorization of the parties to those communications.

30. Until August 2011, Plaintiff used and maintained an HTC cellular phone.

31. Plaintiff and Class Members, as defined below, were unaware of Defendants' wrongful conduct, and unable to discover it until December 2011, as Defendants conduct by nature was secret and concealed.

CLASS ACTION ALLEGATIONS

32. This action is brought as a class action by Plaintiff on behalf of herself and on behalf of all those similarly situated pursuant to Rule 23(a) and 23(b)(1), (2), and (3) of the Federal Rules of Civil Procedure. The proposed class is defined as follows:

All United States residents who operate a cellular phone device manufactured by HTC and from which Carrier IQ, Inc. collected electronic communications (the "Class" or "Class Members").

Specifically excluded from the class are: any Judge conducting proceedings in this action and their parents, spouses and children as well as any other member of their family residing in the judge's household; counsel of record in this action; the legal representatives, heirs, successors and assigns of any excluded person.

33. The exact number of the members of the class (or sub-classes) is not presently known, but is so numerous that joinder of individual members in this action is impracticable. The exact number of the members of the class (or sub-classes) can only be ascertained through discovery, because such information is in the exclusive control of Defendants. However, based on the nature of the activities alleged herein, Plaintiff

believes that the members of the class (or sub-classes) number the millions and are geographically dispersed throughout the United States. The addresses of the members of the class (or sub-classes) are readily obtainable from the Defendants and their agents and on information and belief are maintained in the computer database of Defendants and are easily retrievable.

34. Plaintiff will fairly and adequately protect the interests of the class (or sub-classes) and has retained counsel that are experienced and capable in class action litigation. Plaintiff understands and appreciates her duties to the class (or sub-classes) under Fed. R. Civ. P. 23 and are committed to vigorously protecting the rights of absent members of the class (or sub-classes).

35. Plaintiff is asserting claims that are typical of the claims of each member of the class (or sub-classes) she seeks to represent, in that the claims of all members of the class (or sub-classes), including Plaintiff, depend upon a showing that the Defendants violated federal law. All claims alleged on behalf of the class (or sub-classes) flow from this conduct as well. Further, there is no conflict between Plaintiff and other members of the class (or sub-classes) with respect to this action.

36. There is a well-defined community of interest in the questions of law and fact involved affecting the parties to be represented. Questions of law and fact arising out of Defendants' conduct are common to all members of the class (or sub-classes), and such common issues of law and act predominate over any questions affecting only individual members of the class (or sub-classes).

37. Common issues of law and fact include, but are not limited to, the following:

- a. Whether the data collected from Plaintiff's cellular phone devices are electronic communications protected by the Federal Wiretap Act;
- b. Whether Defendants' interception of data collected from Plaintiff's devices was intentional within the meaning of the Federal Wiretap Act;
- c. The proper measure of damages under the Federal Wiretap Act.

38. The relief sought is common to the entirety of the class (or sub-classes).

39. Defendants have acted on grounds generally applicable to the class (or sub-classes), thereby making final injunctive relief or corresponding injunctive relief appropriate with respect to the class (or sub-classes) as a whole.

40. This action is properly maintained as a class action in that the prosecution of separate actions by individual members would create a risk of adjudication with respect to individual members which would establish incompatible standards of conduct for the Defendants.

41. This action is properly maintained as a class action in that the prosecution of separate actions by individual members of the class (or sub-classes) would create a risk of adjudications with respect to individual members of each class (or sub-classes) which would, as a practical matter, be dispositive of the interests of the other members not parties to the adjudication, or would substantially impair or impede their ability to protect their interests.

42. A class action is superior to other available methods for the fair and efficient adjudication of the claims asserted herein given that, among other things:

- (i) significant economies of time, effort, and expense will inure to the benefit of the Court and the parties in litigating the common issues on a class-wide instead of a repetitive individual basis;
- (ii) the size of the individual damage claims of most members of the class (or sub-classes) is too small to make individual litigation an economically viable alternative, such that few members of the class (or sub-classes) have any interest in individually controlling the prosecution of a separate action;
- (iii) without the representation provided by Plaintiff herein, few, if any, members of the class (or sub-classes) will receive legal representation or redress for their injuries;
- (iv) class treatment is required for optimal deterrence;
- (v) despite the relatively small size of the claims of many individual members of the class (or sub-classes), their aggregate volume coupled with the economies of scale inherent in litigating similar claims on a common basis, will enable this case to be litigated as a class action on a cost effective basis, especially when compared with respective individual litigation;
- (vi) no unusual difficulties are likely to be encountered in the management of this class action;
- (vii) Plaintiff and members of the class (or sub-classes) have all suffered irreparable harm and damages as a result of Defendants' unlawful and wrongful conduct.

43. Concentrating this litigation in one forum would aid judicial economy and efficiency, promote parity among the claims of the individual members of the class (or sub-classes), and result in judicial consistency.

COUNT I

44. Plaintiff incorporates the allegations contained in Paragraphs 1 through 41 as if fully set out herein.

45. The Omnibus Crime Control and Safe Streets Act of 1968, also known as the Federal Wiretap Act, 18 U.S.C. § 2511(1)(e) provides:

[A]ny person who-- ... intentionally intercepts, endeavors to intercept, ... any wire, oral, or electronic communication; ... shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

46. At all times relevant hereto, Plaintiff and Class Members were persons entitled to the protection of 18 U.S.C. § 2511 as they were individuals who were party to electronic communications.

47. On information and belief, Defendants intercepted information concerning the substance, purport, or meaning of Plaintiff's electronic communications on more than one occasion.

48. The Federal Wiretap Act also provides that:

[A]ny person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity ... which engaged in that violation such relief as may be appropriate.

In an action under this section, appropriate relief includes -- ... (2) damages under subsection (c) and punitive damages in appropriate cases; and (3) a reasonable attorney's fee and other litigation costs reasonably incurred ... [T]he court may assess as damages whichever is the greater of -- (A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or (B)

statutory damages of whichever is the greater of \$100 a day for each violation or \$10,000.

18 U.S.C. § 2520

WHEREFORE, Plaintiff and the Class pray that the Court enter judgment in their favor and against Defendants as follows:

- a. Ordering that this action be maintained as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure; and
- b. Declaring that Defendants' collection of electronic communications violates 18 U.S.C. § 2511; and
- c. Awarding Plaintiff and Class Members statutory damages pursuant to 18 U.S.C. § 2520, including punitive damages, costs of suit, and attorneys' fees; and
- d. Injunctive and declaratory relief as deemed appropriate.

Respectfully submitted,

Date: December 8, 2011

Michael M. Weinkowitz

LEVIN, FISHER, SEDRAN & BERMAN

Michael M. Weinkowitz

Charles E. Schaffer

510 Walnut Street, Suite 500

Philadelphia, PA 19106-3697

Telephone: (215)592-1500

Facsimile: (215)592-4663

Email: cschaffer@lfsblaw.com

mweinkowitz@lfsblaw.com

RODDY KLEIN & RYAN

Gary Klein

Shennan Kavanagh

Kevin Costello

727 Atlantic Avenue

Boston, MA 02111-2810
Telephone: (617) 357-5500 ext. 15
Facsimile: (617) 357-5030
Email: klein@roddykleinryan.com
kavanagh@roddykleinryan.com
costello@roddykleinryan.com

HOLLAND, GROVES, SCHNELLER
& STOLZE, LLC
Eric D. Holland, #6207110
Steven J. Stolze, #6203254
Steven L. Groves, #6211737
300 N Tucker, Suite 801
St. Louis, Missouri 63101
Telephone: 314.241.8111
Facsimile: 314.241.5554
Email: eholland@allfela.com
stevenstolze@sbcglobal.net
sgroves@allfela.com

BOLEN, ROBINSON & ELLIS, LLP
Jon D. Robinson
Christopher M. Ellis
Shane M. Mendenhall
202 South Franklin Street, 2nd Floor
Decatur, Illinois 62523
Telephone: 217.429.4296
Facsimile: 217.329.0034
Email: jrobinson@brelaw.com
cellis@brelaw.com
smendenhall@brelaw.com

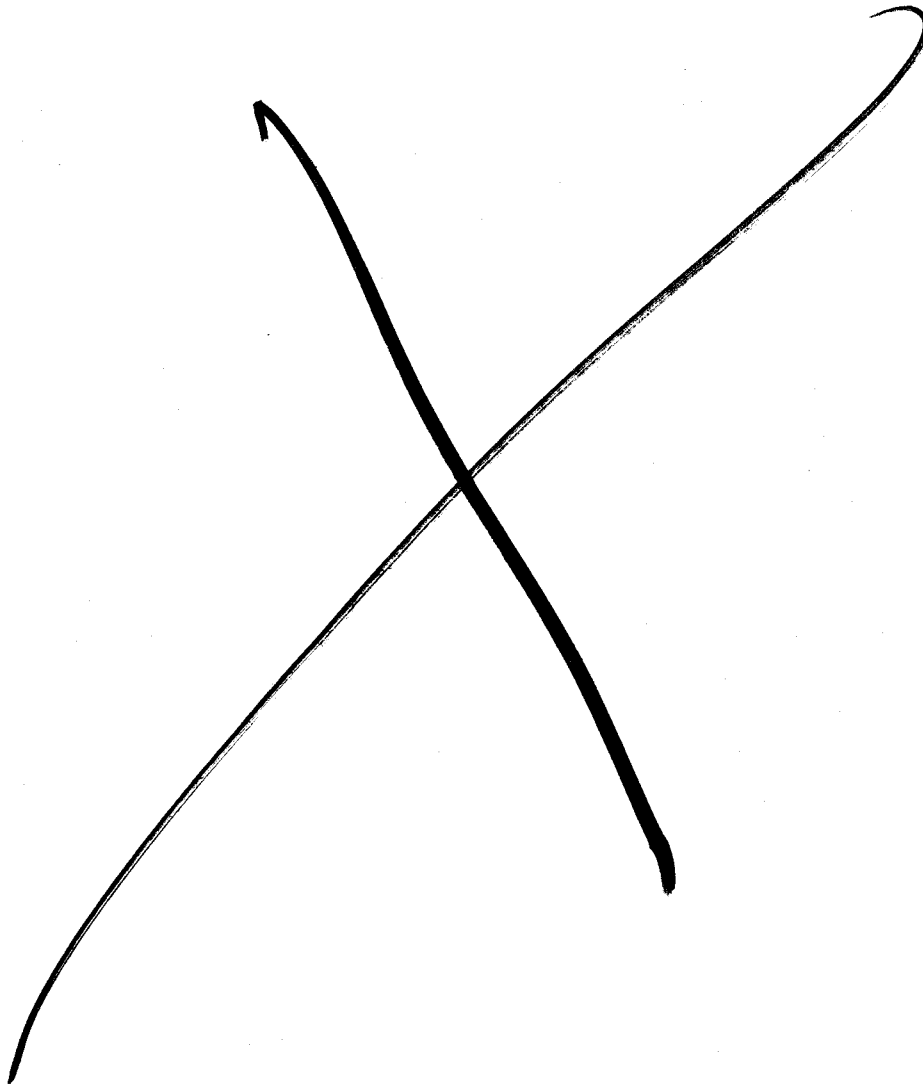


Exhibit 6:

***Accident Investigative Services, Inc. v.
Carrier IQ, Inc., et al.***

SPECIAL

**United States District Court
Eastern District of Pennsylvania (Philadelphia)
CIVIL DOCKET FOR CASE #: 2:11-cv-07542-TJS**

ACCIDENT INVESTIGATIVE SERVICES, INC. v. CARRIER IQ, INC. et al Date Filed: 12/08/2011
Assigned to: HONORABLE TIMOTHY J. SAVAGE Jury Demand: Plaintiff
Cause: 18:2511 Wiretapping Nature of Suit: 440 Civil Rights: Other
Jurisdiction: Federal Question

Plaintiff

**ACCIDENT INVESTIGATIVE
SERVICES, INC.
INDIVIDUALLY, AND ON BEHALF OF
ALL OTHERS SIMILARLY SITUATED**

represented by **CHARLES E. SCHAFER**
**LEVIN, FISHBEIN, SEDRAN
&BERMAN**
510 WALNUT STREET
SUITE 500
PHILADELPHIA, PA 19106
215-592-1500
Email: cschaffer@lfsblaw.com
ATTORNEY TO BE NOTICED

V.

Defendant

CARRIER IQ, INC.

Defendant

HTC, INC.

Defendant

HTC AMERICA, INC.

Date Filed	#	Docket Text
12/08/2011	<u>1</u>	COMPLAINT against CARRIER IQ, INC., HTC AMERICA, INC., HTC, INC. (Filing fee \$ 350 receipt number 054341.), filed by ACCIDENT INVESTIGATIVE SERVICES, INC..(mima,) (Entered: 12/08/2011)
12/08/2011		Summons Issued as to CARRIER IQ, INC., HTC AMERICA, INC., HTC, INC.. Forwarded To: Counsel on December 8, 2011 (mima,) (Entered: 12/08/2011)
12/08/2011		DEMAND for Trial by Jury by ACCIDENT INVESTIGATIVE SERVICES, INC.. (mima,) (Entered: 12/08/2011)

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON THE REVERSE OF THE FORM.)

I. (a) PLAINTIFFS

ACCIDENT INVESTIGATIVE SERVICES, INC.,
individually, and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff Montgomery County PA
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorney's (Firm Name, Address, and Telephone Number)

Charles E. Schaffer, Levin, Fishbein, Sedran & Berman, 510
Walnut Street, Suite 500, Philadelphia, PA 19106 (215) 592-1500

DEFENDANTS

CARRIER IQ, INC., HTC, INC., & HTC AMERICA, INC.

County of Residence of First Listed Defendant Cook County, IL
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE
LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box)

- ☐ 1 U.S. Government Plaintiff ☒ 3 Federal Question (U.S. Government Not a Party)
- ☐ 2 U.S. Government Defendant ☐ 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Defendant and One Box for Plaintiff)

- (For Diversity Cases Only)
- | PTF | DEF | PTF | DEF |
|---|---------------------------------------|--|--|
| Citizen of This State | <input checked="" type="checkbox"/> 1 | <input type="checkbox"/> 1 Incorporated or Principal Place of Business In This State | <input type="checkbox"/> 4 <input type="checkbox"/> 4 |
| Citizen of Another State | <input type="checkbox"/> 2 | <input type="checkbox"/> 2 Incorporated and Principal Place of Business In Another State | <input type="checkbox"/> 5 <input checked="" type="checkbox"/> 5 |
| Citizen or Subject of a Foreign Country | <input type="checkbox"/> 3 | <input type="checkbox"/> 3 Foreign Nation | <input type="checkbox"/> 6 <input type="checkbox"/> 6 |

IV. NATURE OF SUIT (Place an "X" in One Box Only)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excl. Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury PERSONAL INJURY <input type="checkbox"/> 362 Personal Injury - Med. Malpractice <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 610 Agriculture <input type="checkbox"/> 620 Other Food & Drug <input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 630 Liquor Laws <input type="checkbox"/> 640 R.R. & Truck <input type="checkbox"/> 650 Airline Regs. <input type="checkbox"/> 660 Occupational Safety/Health <input type="checkbox"/> 690 Other LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Mgmt. Relations <input type="checkbox"/> 730 Labor/Mgmt. Reporting & Disclosure Act <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Empl. Ret. Inc. Security Act IMMIGRATION <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 463 Habeas Corpus - Alien Detainee <input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 PROBATE RIGHTS <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 840 Trademark SOCIAL SECURITY <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	<input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 810 Selective Service <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 875 Customer Challenge 12 USC 3410 <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 892 Economic Stabilization Act <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 894 Energy Allocation Act <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 900 Appeal of Fee Determination Under Equal Access to Justice <input type="checkbox"/> 950 Constitutionality of State Statutes
REAL PROPERTY <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	CIVIL RIGHTS <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 444 Welfare <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input checked="" type="checkbox"/> 440 Other Civil Rights	PRISONER PETITIONS <input type="checkbox"/> 510 Motions to Vacate Sentence Habeas Corpus: <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition		

V. ORIGIN

(Place an "X" in One Box Only)

- ☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from another district (specify) ☐ 6 Multidistrict Litigation ☐ 7 Appeal to District Judge from Magistrate Judgment

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):

18 U.S.C. Section 2511, 28 U.S.C. Sections 1331 and 1332(d)

Brief description of cause:

Violation of Wiretap Act by illegally gathering electronic data

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A CLASS ACTION UNDER F.R.C.P. 23

DEMAND \$

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE

DOCKET NUMBER

DATE

12/08/2011

SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

RECEIPT #

AMOUNT

APPLYING IF

JUDGE

MAG. JUDGE

JS 44 Reverse (Rev. 12/07)

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

Case 3:11-cv-03483-M Document 7 Filed 12/23/11 Page 50 of 153 PageID 176
The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I. (a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.C.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.

United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.

United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.

Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; federal question actions take precedence over diversity cases.)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerks in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. Origin. Place an "X" in one of the seven boxes.

Original Proceedings. (1) Cases which originate in the United States district courts.

Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.

Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

Multidistrict Litigation. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407. When this box is checked, do not check (5) above.

Appeal to District Judge from Magistrate Judgment. (7) Check this box for an appeal from a magistrate judge's decision.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. Do not cite jurisdictional statutes unless diversity. Example: U.S. Civil Statute: 47 USC 553
Brief Description: Unauthorized reception of cable service

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.

Demand. In this space enter the dollar amount (in thousands of dollars) being demanded or indicate other demand such as a preliminary injunction.

Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related pending cases if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

CASE MANAGEMENT TRACK DESIGNATION FORM

Accident Investigative Services, Inc., individually, :
and on behalf of all others similarly situated : CIVIL ACTION
v. :
Carrier IQ, Inc., HTC, Inc. and HTC America, Inc. : NO.

In accordance with the Civil Justice Expense and Delay Reduction Plan of this court, counsel for plaintiff shall complete a Case Management Track Designation Form in all civil cases at the time of filing the complaint and serve a copy on all defendants. (See § 1:03 of the plan set forth on the reverse side of this form.) In the event that a defendant does not agree with the plaintiff regarding said designation, that defendant shall, with its first appearance, submit to the clerk of court and serve on the plaintiff and all other parties, a Case Management Track Designation Form specifying the track to which that defendant believes the case should be assigned.

SELECT ONE OF THE FOLLOWING CASE MANAGEMENT TRACKS:

- (a) Habeas Corpus – Cases brought under 28 U.S.C. § 2241 through § 2255. ()
- (b) Social Security – Cases requesting review of a decision of the Secretary of Health and Human Services denying plaintiff Social Security Benefits. ()
- (c) Arbitration – Cases required to be designated for arbitration under Local Civil Rule 53.2. ()
- (d) Asbestos – Cases involving claims for personal injury or property damage from exposure to asbestos. ()
- (e) Special Management – Cases that do not fall into tracks (a) through (d) that are commonly referred to as complex and that need special or intense management by the court. (See reverse side of this form for a detailed explanation of special management cases.) (✓)
- (f) Standard Management – Cases that do not fall into any one of the other tracks. ()

12/08/2011
Date

Charles E. Schaffer
Attorney-at-law

Plaintiff
Attorney for

(215) 592-1500
Telephone

(215) 592-4663
FAX Number

CSchaffer@lfsblaw.com
E-Mail Address

**Civil Justice Expense and Delay Reduction Plan
Section 1:03 - Assignment to a Management Track**

- (a) The clerk of court will assign cases to tracks (a) through (d) based on the initial pleading.
- (b) In all cases not appropriate for assignment by the clerk of court to tracks (a) through (d), the plaintiff shall submit to the clerk of court and serve with the complaint on all defendants a case management track designation form specifying that the plaintiff believes the case requires Standard Management or Special Management. In the event that a defendant does not agree with the plaintiff regarding said designation, that defendant shall, with its first appearance, submit to the clerk of court and serve on the plaintiff and all other parties, a case management track designation form specifying the track to which that defendant believes the case should be assigned.
- (c) The court may, on its own initiative or upon the request of any party, change the track assignment of any case at any time.
- (d) Nothing in this Plan is intended to abrogate or limit a judicial officer's authority in any case pending before that judicial officer, to direct pretrial and trial proceedings that are more stringent than those of the Plan and that are designed to accomplish cost and delay reduction.
- (e) Nothing in this Plan is intended to supersede Local Civil Rules 40.1 and 72.1, or the procedure for random assignment of Habeas Corpus and Social Security cases referred to magistrate judges of the court.

**SPECIAL MANAGEMENT CASE ASSIGNMENTS
(See §1.02 (e) Management Track Definitions of the
Civil Justice Expense and Delay Reduction Plan)**

Special Management cases will usually include that class of cases commonly referred to as "complex litigation" as that term has been used in the Manuals for Complex Litigation. The first manual was prepared in 1969 and the Manual for Complex Litigation Second, MCL 2d was prepared in 1985. This term is intended to include cases that present unusual problems and require extraordinary treatment. See §0.1 of the first manual. Cases may require special or intense management by the court due to one or more of the following factors: (1) large number of parties; (2) large number of claims or defenses; (3) complex factual issues; (4) large volume of evidence; (5) problems locating or preserving evidence; (6) extensive discovery; (7) exceptionally long time needed to prepare for disposition; (8) decision needed within an exceptionally short time; and (9) need to decide preliminary issues before final disposition. It may include two or more related cases. Complex litigation typically includes such cases as antitrust cases; cases involving a large number of parties or an unincorporated association of large membership; cases involving requests for injunctive relief affecting the operation of large business entities; patent cases; copyright and trademark cases; common disaster cases such as those arising from aircraft crashes or marine disasters; actions brought by individual stockholders; stockholder's derivative and stockholder's representative actions; class actions or potential class actions; and other civil (and criminal) cases involving unusual multiplicity or complexity of factual issues. See §0.22 of the first Manual for Complex Litigation and Manual for Complex Litigation Second, Chapter 33.

FOR THE EASTERN DISTRICT OF PENNSYLVANIA — DESIGNATION FORM to be used by counsel to indicate the category of the case for the purpose of assignment to appropriate calendar.

Address of Plaintiff: 222 Easton Road, Glenside, PA 19038

Address of Defendant: 200 West Adams Street, Chicago, IL 60606

Place of Accident, Incident or Transaction: Pennsylvania

(Use Reverse Side For Additional Space)

Does this civil action involve a nongovernmental corporate party with any parent corporation and any publicly held corporation owning 10% or more of its stock?

(Attach two copies of the Disclosure Statement Form in accordance with Fed.R.Civ.P. 7.1(a))

Yes ☐ No ☒

Does this case involve multidistrict litigation possibilities?

Yes ☒ No ☐

RELATED CASE, IF ANY:

Case Number: _____ Judge _____ Date Terminated: _____

Civil cases are deemed related when yes is answered to any of the following questions:

1. Is this case related to property included in an earlier numbered suit pending or within one year previously terminated action in this court?
Yes ☐ No ☐
2. Does this case involve the same issue of fact or grow out of the same transaction as a prior suit pending or within one year previously terminated action in this court?
Yes ☐ No ☐
3. Does this case involve the validity or infringement of a patent already in suit or any earlier numbered case pending or within one year previously terminated action in this court?
Yes ☐ No ☐
4. Is this case a second or successive habeas corpus, social security appeal, or pro se civil rights case filed by the same individual?
Yes ☐ No ☐

CIVIL: (Place ☒ in ONE CATEGORY ONLY)

A. Federal Question Cases:

1. ☐ Indemnity Contract, Marine Contract, and All Other Contracts
2. ☐ FELA
3. ☐ Jones Act-Personal Injury
4. ☐ Antitrust
5. ☐ Patent
6. ☐ Labor-Management Relations
7. ☐ Civil Rights
8. ☐ Habeas Corpus
9. ☐ Securities Act(s) Cases
10. ☐ Social Security Review Cases
11. ☒ All other Federal Question Cases
(Please specify) - Violation of Wiretap Act by illegally gathering electronic data

B. Diversity Jurisdiction Cases:

1. ☐ Insurance Contract and Other Contracts
2. ☐ Airplane Personal Injury
3. ☐ Assault, Defamation
4. ☐ Marine Personal Injury
5. ☐ Motor Vehicle Personal Injury
6. ☐ Other Personal Injury (Please specify)
7. ☐ Products Liability
8. ☐ Products Liability — Asbestos
9. ☒ All other Diversity Cases
(Please specify) - Violation of Wiretap Act by illegally gathering electronic data

ARBITRATION CERTIFICATION

(Check Appropriate Category)

I, Charles E. Schaffer

counsel of record do hereby certify:

- X Pursuant to Local Civil Rule 53.2, Section 3(c)(2), that to the best of my knowledge and belief, the damages recoverable in this civil action case exceed the sum of \$150,000.00 exclusive of interest and costs;
- X Relief other than monetary damages is sought.

DATE: 12/08/2011

Attorney-at-Law

76259

Attorney I.D.#

NOTE: A trial de novo will be a trial by jury only if there has been compliance with F.R.C.P. 38.

I certify that, to my knowledge, the within case is not related to any case now pending or within one year previously terminated action in this court except as noted above.

DATE: 12/08/2011

Attorney-at-Law

76259

Attorney I.D.#